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

студента Сорокопуд Єгор Максимович
(ПІБ)
академічної групи 123-20-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему "Кіберфізична система комп'ютерного клубу на базі програмно-конфігурованих мереж з використанням технологій Інтернету речей"
(назва за наказом ректора)

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

Дніпро
2024

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Сорокопуд Є.М. **академічної групи** 123-20-1
(прізвище та ініціали) (шифр)

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

на тему «Кіберфізична система комп'ютерного клубу на базі прогсрамно-конфігурованих мереж з використанням технологій Інтернету речей»
затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання програмно-конфігурованих мереж	05.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою, розробити структурну схему та специфікацію обладнання.	12.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель мережі розумного будинку, виконати налаштування та перевірку роботи системи.	30.05.2024
Розробка компонента системи	Реалізувати та налаштувати систему моніторингу температури в розумному будинку з використаням програмно-конфігурованих мереж	20.06.2024

Завдання видано _____ доц. Сергєєва К.Л.
(підпис керівника) (прізвище, ініціали)

Дата видачі 06.02.2024

Дата подання до екзаменаційної комісії 01.07.2024

Прийнято до виконання _____ Сорокопуд Є.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 80 с., 28 рис., 7 таблиць., 12 джерел.

КІБЕРФІЗИЧНА СИСТЕМА, ЩО ПІДВИЩУЄ ЯКІСТЬ ПОСЛУГ ТА КОНТРОЛЬ МІКРОКЛИМАТУ КОМП'ЮТЕРНОГО КЛУБУ «СКАЛА»

Метою розробки є кіберфізична система для моніторингу та управління процесами обслуговування клієнтів у комп'ютерному клубі «СКАЛА» (з використанням моделювання в packet tracers).

Метою даної роботи є створення системи автоматичного контролю і управління мікро клімату, з метою підвищення послуг комп'ютерного клубу «СКАЛА» з використанням IT-технологій.

Була розроблена комп'ютерна мережа з використанням вимірювальних пристроїв, таких як датчики температури, рівня вологості та мережеві монітори. Система орієнтована на забезпечення високої якості обслуговування клієнтів у будь-якому комп'ютерному клубі.

Створена кіберфізична система не тільки дозволяє модернізувати технологію і програмне забезпечення, але й надає наступні можливості:

Онлайн і оффлайн моніторинг стану обладнання та умов у приміщеннях клубу;

Автоматичне налаштування параметрів для оптимального функціонування обладнання;

Забезпечення безпеки і якості послуг для клієнтів.

Розроблена комп'ютерна мережа виконується відповідно до завдання на виконання кваліфікаційної роботи бакалавра.

Поведінка системи була перевірена за допомогою моделі схеми корпоративної мережі за допомогою програми Cisco Packet Tracer.

Результати перевірки у вигляді таблиць і графіків можна знайти в пояснювальному тексті і додатку

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

LAN (Local Area Network) - локальна мережа

WAN (Wide Area Network) - глобальна мережа

IP (internet Protocol) - інтернет-протокол

MAC (Media Access Control) - контроль доступу до середовища

CPU (Central Processing Unit) - центральний процесор

RAM (Random Access Memory) - оперативна пам'ять

HDD (Hard Disk Drive) - жорсткий диск

SSD (Solid State Drive) - твердотільний накопичувач

VPN (Virtual Private Network) - віртуальна приватна мережа

ISP (Internet Service Provider) - інтернет-провайдер

QoS (Quality of Service) - якість обслуговування

DNS (Domain Name System) - система доменних імен

DHCP (Dynamic Host Configuration Protocol) - протокол динамічної конфігурації вузлів

TCP/IP (Transmission Control Protocol/Internet Protocol) - протокол управління передачею/інтернет-протокол

FTP (File Transfer Protocol) - протокол передачі файлів

HTTP (HyperText Transfer Protocol) - протокол передачі гіпертексту

SSID (Service Set Identifier) - ідентифікатор набору послуг (назва Wi-Fi мережі)

MTTR (Mean Time To Repair) - Середній час на відновлення, який потрібен для того, щоб відновити систему

IoT (Internet of Things) - інтернет речей

UPS (Uninterruptible Power Supply) - джерело безперебійного живлення

RDP (Remote Desktop Protocol) - протокол віддаленого робочого столу

WLAN (Wireless Local Area Network) - бездротова локальна мережа

CLI (Command Line Interface) - командний інтерфейс

ВСТУП

У нашому світі, де інформаційні технології відіграють ключову роль у функціонуванні будь-якої галузі, особливо важливою стає розробка ефективної та безпечної моделі комп’ютерної мережі. Комп’ютерний клуб "СКАЛА", як технологічний центр, що надає широкий спектр послуг з обміну персональнмх, технічних даних та забезпечення комунікації між відділами клубу, потребує сучасних рішень для підтримки своєї діяльності.

Головною метою цієї роботи є проектування безпечної та ефективної комп’ютерної мережі для комп'ютерного клубу "СКАЛА". Це передбачає забезпечення надійного обміну даними між відділами, встановлення зв’язку з віддаленими сервісами та філіями, а також впровадження системи на основі IoT пристроїв.

У цій роботі буде розглянуто можливі напрямки вирішення поставлених завдань, що дозволить створити ефективну та безпечну мережу, яка відповідає сучасним стандартам та потребам.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної мережі

Галузь інформаційних технологій та розваг осягає різноманітні сегменти, що охоплюють як інформаційні технології так і розважальну індустрію. Ця галузь постійно зростає та розширується, що віддзеркалюється у швидкісних технологічних змінах та впровадження нововведень.

Зараз, завдяки постійному доступу до Інтернету, нам не потрібно відвідувати бібліотеки для пошуку інформації. Підприємства також активно використовують комп'ютери та Інтернет для збору, зберігання та обміну інформацією, що дозволяє їм уникати залежності від паперової документації та традиційних засобів зберігання.

Інформаційні технології включають в себе розробку програмного забезпечення, ОС, мережі зв'язку та бази даних. Розважальна галузь включає в себе компьютерні ігри, кіно, телебачення, музику та інші забави.

В основі своїй ІТ та розважальні технології відомі своєю технологічною інноваційністю, що приводить до появи нових продуктів та послуг бо ця сфера є дуже популярною та конкурентно здатною, що вимагає від компаній постійно шукати способи відрізнятися від конкурентів.

Також не треба забувати що Технології постійно розвиваються, що вимагає від фахівців у цій галузі постійного навчання та адаптації до нових тенденцій. Галузь має обширну базу знаннь, яка сприяє співпраці та конкуренції між компаніями, ця конкуренція спонукає розвиватися та вдосконаливати вже існуючи технології.

Інформаційні технології та розважальні технології значно впливають на суспільство, змінюючи способи комунікації, розваг та роботи. В умовах, коли технології стають неот'ємною частиною нашого повсякденного життя, захист

інформації та персональних даних стає все більш важливим, що вимагає від представникив тих чи інших галузей витрачатися на новітні способи захисту персональних данних.

Протягом останніх десятиліть спостерігається зростання попиту на продукти та послуги в галузі інформаційних технологій та розваг, що робить цей сектор одним із найдинамічніших та перспективних. Розваги та новітнні технології настільки стали не відлучною від життя звичайної людини що вже не уявляєш її без них.

Розвинення інформаційних технологій суттєво вплинув на розвиток розважальної галузі, Телебачення, відео ігор, стримінгових сервісів, музикальні сервіси та кіно, ці технології стали невідлучною складовою сучасного розважального світу, без яких важко уявити собі наш час. Інформаційні технології мають величезний потенціал для подальшого удосконалення у розважальній галузі, відкриваючи нові можливості для творчості та споживання контенту. Однак, разом з цим, важливо забезпечити безпеку даних споживачів, оскільки без належної захисту не можна гарантувати безпечність їх особистої інформації. Майбутній розвиток розважальної галузі буде залежати від споживачів, які визначають тренди сучасності.

1.2 Характеристика і структура об’єкта впровадження

Комп'ютерний клуб "СКАЛА" розпочав свою роботу у грудні 2001 року за адресою просп. Коцюбинского, 38в. У початковому вигляді у клубі було 10 місць для сидіння. Поступово клуб розширився до 25 місць у ігровому залі та 16 місць у інтернет-залі.

У 2002 році, з самого початку формування кіберспорту, Клуб орієнтувався як місце для обслуговування клієнтів, проведення турнірів та тренувань команд. Організовувалися змагання з різних видів ігор, а з 2004 року “СКАЛА” є членами Асоціації комп'ютерних клубів України, яка суттєво допомагає надавати більш стабільні та якісні послуги для користувачив.

Зокрема, комп'ютерний клуб "СКАЛА" активно використовує сучасні інформаційні технології для організації електронних кабінетів користувачив, що дозволяє поліпшити ефективність та безпеку за надання різноманітних послуг. Інформаційні системи, такі як GameSys або CyberCafePro, надають можливість автоматизувати роботу комп'ютерних клубів, широкий спектр функцій для управління клієнтами, контролю доступу до інтернету, моніторингу комп'ютерів та автоматизації фінансових операцій.

В клубі працюють адміністратори, системні адміністратори, фінансові менеджери, інструктора, технічний спеціалісти з разник галузей та ще багато інщих фахівців які надають ефективні та якісні послуги. Кожна з цих професій відіграє важливу роль у забезпеченні ефективної роботи комп'ютерного клубу за для задоволення потреб клієнтів.

Комп’ютери оснащени сучасним обладнанням та системним ПЗ.

Сьогодні клуб продовжує розвиватися та вдосконалювати свої послуги, зосереджуючись на забезпеченні найвищих стандартів у сфері розважального обслуговування. Крім того, повністю перебудували головну залу, ігровий зал та побудову клубу.

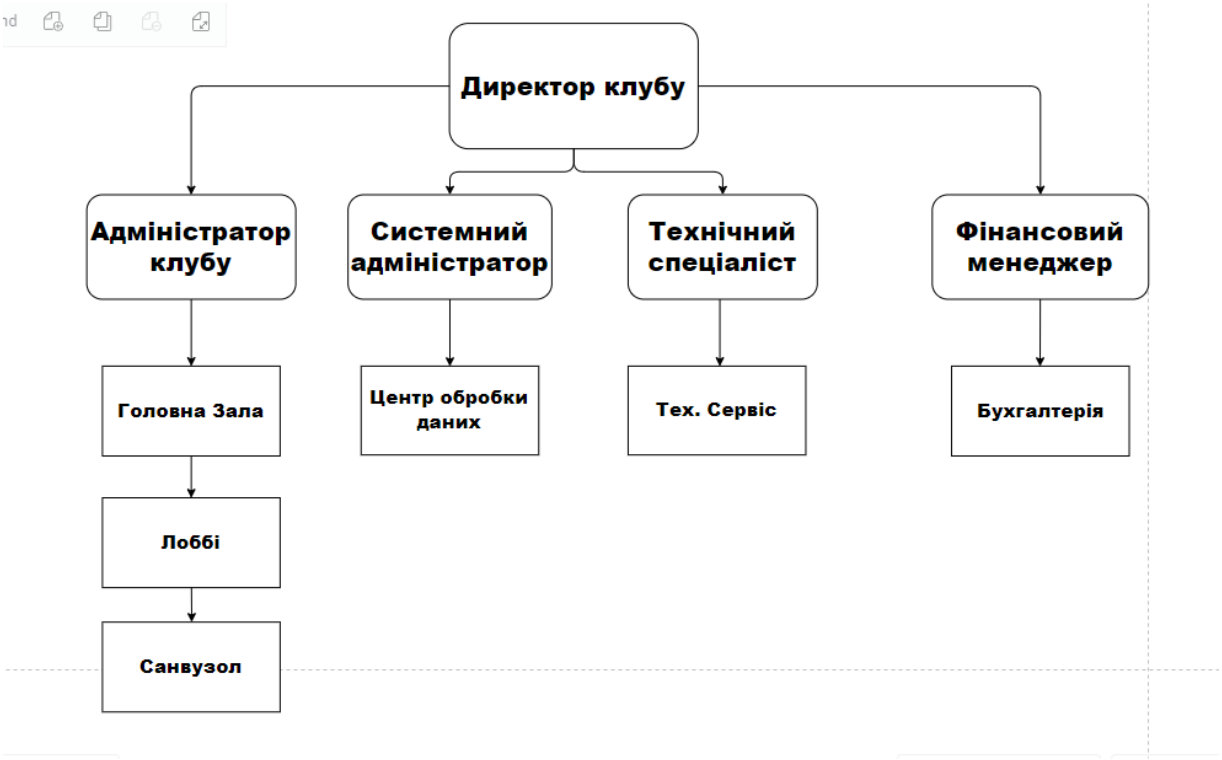

Рисунок 1.1 – Організаційної структури підприємства

Об’єкт впровадження комп’ютерної мережі знаходиться за юридичною адресою: просп. Коцюбинского, 38в ТЦ ”СВ” м. Вінниця, Вінницька область.

Рисунок 1.2 – Схема гео-позиції «комп'ютерный клуб ”СКАЛА”»

1.3 Стислі відомості про технологію керування для об’єкта впровадження

Топологія комп’ютерного клубу «СКАЛА» складається з головної будівлі, яка складається з самого клубу на другому поверсі та кафе на першому поверсі (який у цьому проекті розглянутий не буде), також зазначемо що цей клуб має філію в який входить ще один клуб.(він не буду розглядатися у цьому проекті).

Топологічна схема розглянутих відділів була побудована спираючись на інформацію, що містилася безпосередньо в основному клубі. Представлена топологія головного зала другого поверху комп’ютерного клубу “СКАЛА”. Центр обробки даних та бухгалтерський відділ представлені на рисунку

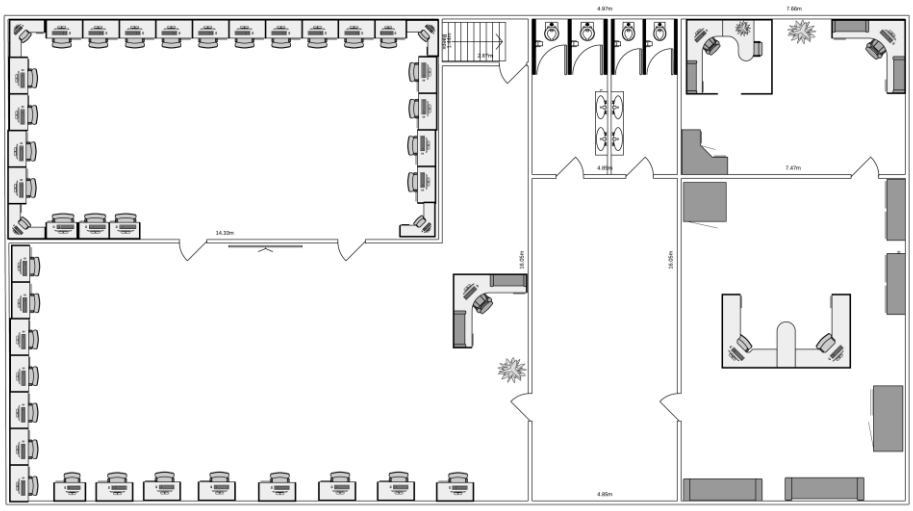

Рисунок 1.3 – Топологія комп’ютерного клубу «СКАЛА»

На другому поверсі ТЦ розташована лоббі клуба “СКАЛА”, гардеробна, підсобне приміщення, пост Адміністратора. Якщо пройти далі то можно побачити головну залу, Бухгалтерський відділ, тех. сервіс представлений серверною, кабінетом головного директора та фінансового менеджера є представлений раніше Бухгалтерський відділ.

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

Проектування ефективної та надійної мережі в закладі потребує використання різних принципів, технічних методів та математичних моделей, щоб забезпечити безперебійний доступ до даних, збереження конфіденційності клієнтів та відповідність усім необхідним стандартам безпеки.

Принципи мережевого проектування:

– сегментація мережі: Поділ мережі на окремі сегменти допомогає ізолювати конфіденційну інформацію та зменшити поширення шкідливих програм;

– створення резервних копій даних та використання резервних шляхів для передачі даних підвищує надійність мережі;

– мережа має бути здатною розширюватися та адаптуватися до зростаючих потреб закладу;

– постійний моніторинг трафіку дозволяє виявляти та запобігати потенційним загрозам.

Технічні методи:

– використання віртуальних приватних мереж (VPN) та шифрування даних підвищує рівень конфіденційності та безпеки передачі даних;

– використання аутентифікації та ролей користувачів для контролю доступу до мережі та даних;

– икористання корпоративної електронної пошти в закладі охорони здоров’я є важливою частиною комунікації між співробітниками та може містити конфіденційну інформацію про пацієнтів.

Математичні методи:

– використання математичних моделей для аналізу пропускної здатності мережі та планування пропускних каналів;

– використання оптимізованих алгоритмів маршрутизації для підвищення ефективності передачі даних;

– застосування математичних моделей для прогнозування навантаження на мережу та оптимізації її роботи.

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

Сфера комп'ютерних клубів активно розвивається завдяки технологічним інноваціям у сфері обробки та передачі інформації. Відомі такі рішення у галузі.

а) Електронні облікові записи клієнтів дозволяють адміністратору та персоналу ефективно зберігати, передавати та обмінюватися даними клієнтів. Електронні облікові записи включають інформацію про відвідування, використаний час, платежі та інші важливі дані.

б) Віддалений доступ дозволяє адміністраторам та технічним

спеціалістам управляти клубом, проводити консультації, діагностику та технічну підтримку через відеозв'язок. Це покращує якість обслуговування, особливо для клубів з кількома філіями або для віддалених користувачів.

в) Інтернет речей (IoT) у комп'ютерних клубах. Пристрої, підключені до інтернету, можуть відстежувати використання обладнання, температурні умови, стан мережі та інші параметри. Ці дані можуть бути передані адміністраторам для моніторингу та оптимізації роботи клубу в реальному часі. Також IoT поширено використовується у системах безпеки.

г) Хмарні технології дозволяють ефективно зберігати та обмінюватися даними клієнтів, налаштуваннями іграми та програмним забезпеченням, а також забезпечувати віддалене управління клубом.

1.6 Мета роботи, що виконується

Мета роботи: Проектування ефективної Кіберфізичної системи в комп’ютерний клуб «СКАЛА» для забезпечення контролю мікро климату та оптимізація рутинних справ. Забезпечити комунікацію з сервісами та філіями. Допоможе впровадження Комп'ютерної системи та з допомогою IoT пристроїв та спеціальних контролерів.

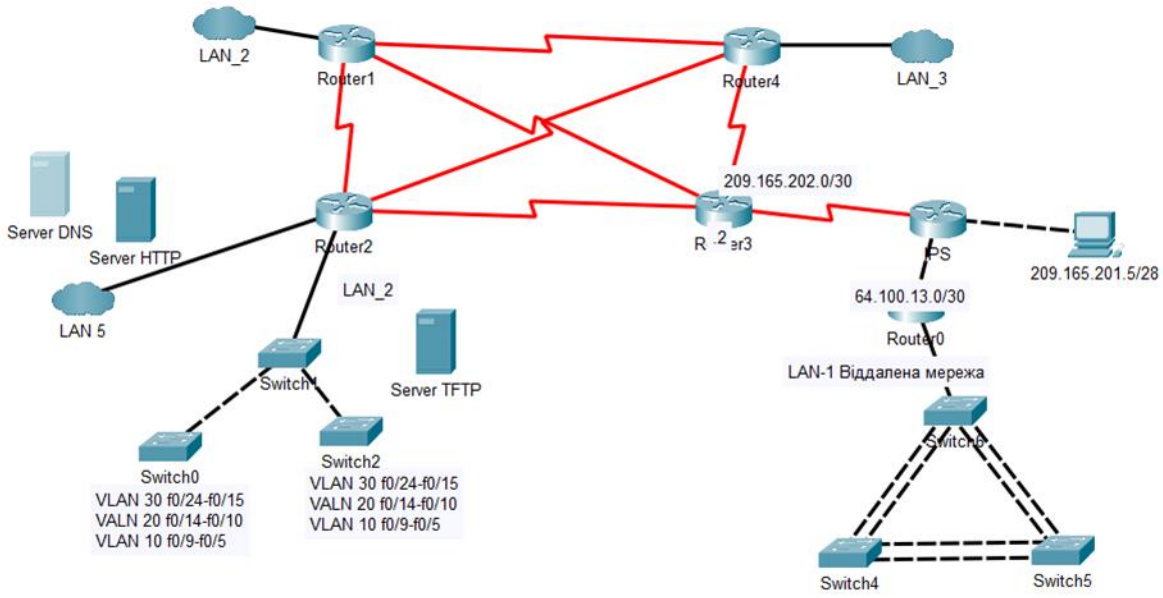

Рисунок 1.4 – Топологія мережі комп’ютерного клубу «СКАЛА»

1.7 Визначення можливих напрямків рішення поставлених завдань.

Кіберфізична система (Cyber-Physical System, CPS) − це інтегрована система, що поєднує в собі обчислювальні (кібер) та фізичні процеси. кіберфізична система (CPS) не може існувати без комп'ютерної системи, оскільки вона інтегрує обчислювальні компоненти з фізичними процесами для моніторингу та управління через мережу. Комп'ютерна система є ключовим елементом, що забезпечує обробку даних, керування та зв'язок в межах кіберфізичної системи. Ці системи забезпечують взаємодію між фізичними об'єктами та комп'ютерними алгоритмами.

Комутатори та маршрутизатори: Вибір обладнання з необхідною пропускною здатністю та функціями безпеки, такими як підтримка VLAN, QoS, та інші.

Серверне обладнання: Вибір серверів для виконання ролей файлівого серверу, серверу додатків, та серверу баз даних

Системи керування мережею: Використання програмного забезпечення для моніторингу, управління та забезпечення безпеки мережі (Cisco Network Assistant.)

Вибір провайдера: Усі приміщення знаходяться на не дуже великій відстані один від одного, тому дуже висока швидкість тут буде зайвою. У місті Вінниця доступно небагато провайдерів: Фрегат, Київстар, Укртелеком та Vodafone. Фрегат та Укртелеком мають дуже погані відгуки, тому обираємо Київстар, так як він має найвищий рейтинг з вказаних вище провайдерів (хоч його показники на 2023-2024 впали, але він всеодно тримає лідуючи позиції.)

Підключення до інформаційної системи CyberCafePro дасть комп'ютерному клубу «СКАЛА» ряд важливих інновацій. Це дозволить автоматизувати управління клубом, включаючи контроль часу використання комп'ютерів клієнтами, автоматизований розрахунок вартості послуг та зручний

облік клієнтів і їхніх платежів. Додатково, система забезпечить покращення безпеки, контролюючи доступ до інтернету та окремих програм, моніторячи діяльність користувачів та захищаючи від несанкціонованого доступу і зломів. Підтримка та технічна допомога від розробників CyberCafePro забезпечать доступ до регулярних оновлень програмного забезпечення, технічної підтримки та навчальних матеріалів для персоналу.

Вибір топології комп’ютерної мережі, враховуючи варіант вектору розвитку корпоративної мережі.

Розробка фізичної та логічної топології корпоративної мережі підприємства.

Налаштування мережевого обладнання через Cisco Packet tracer.

Використання контролерів та шоломів віртуальної реальності.

1.8 Обґрунтування вибраного напрямку інженерного рішення.

Комп’ютерна мережа клубу «СКАЛА» має віддалену філію. Філія “СКАЛА” має підрозділи, яким не потрібне високошвидкісне з’єднання з головними відділами, бо він є автономним. До її складу входять такіж самі групи що і у основого комплексу.

CyberCafePro надає клієнтам можливість швидко та зручно забронювати комп'ютери, отримати доступ до ігор та програм, оплачувати послуги, а також замовляти додаткове обладнання та послуги.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до Системи

Кіберфізична система повинна бути інтегрована у комп'ютерною систему, оскільки вона виконує обчислювальні компоненти з фізичними процесами для моніторингу та управління через мережу. Комп'ютерна система є ключовим елементом, що забезпечує обробку даних, керування та зв'язок в межах кіберфізичної системи. Система повинна забезпечувати взаємодію між фізичними об'єктами та комп'ютерними алгоритмами, а для персоналу клубу оптимізувати рутинні справи та забезпечити надійний джерело інформації про стан комп'ютерного клубу. У головній ігровій залі мають бути розташовувані основна частиua Інтернету речей (IoT), що об'єднує датчики (температури, фільтрації повітря, музикальні станції). Впровадити ігрові периферійні пристрої (рисунки 2.1, 2.2, 2.3) , які забезпечать максимальне занурення у комп'ютерні ігри або будь-які інші симулятори.

Рисунок 2.1 – Контролери для машинних симуляторів

Рисунок 2.2 – Контролери для польотних симуляторів

Рисунок 2.3 – VR-шолом

За для забеспечення оптимізованого управління, та росподілу навантаження створили сигментовану мережу яка має такі переваги як:

– адміністрування кожної підмережі здійснюється окремо, що спрощує обслуговування, підвищує ефективність роботи мережі та допомагає оптимізувати рутинні завдання»

– можливість впровадження окремих політик безпеки для кожної підмережі (VPN, Фаєрволів) знижує ризики несанкціонованого доступу та зливу персональних даних користувачів;

– локалізація трафіку в межах підмереж знижує навантаження на основні канали зв'язку, забезпечуючи швидшу передачу даних і, таким чином, підвищуючи пропускну здатність;

– архітектура мережі забезпечує легке додавання нових вузлів та підмереж відповідно до потреб клубу.

Структура мережі комп'ютерного клубу "СКАЛА"

LAN_1 – Технічний сервіс

LAN_2 – Головна ігрова зала

LAN_3 – Зовнішня ігрова зала

LAN_4 – Лоббі

LAN_5 – Бухгалтерія

2.1.1 Вимоги до структури і функціонування Кіберфізичної системи

Структура системи повинна включати носій (ПК), на якому створюватиметься з'єднання кібер та фізичної систем, який відповідатиме за

управління конкретною станцією. На кожному комп'ютері повинне бути встановлено програмне забезпечення CyberCafePro для контроля доступу.

ПЗ повинна забезпечувати реєстрацію користувачів, контроль часу сеансу, надання доступу до комп'ютерів та моніторинг активності, це все буде виконувати софт CyberCafePro який значно полегчить роботу в клубі.

Підтримка локальних та віртуальних локальних мереж

На основі наданої інформації про структуру системи, вона буде реалізована в застосуванні протоколу динамічної маршрутизації OSPF для автоматичного визначення та оновлення маршрутів між підмережами сприятиме оптимальній доставці пакетів і покращить ефективність функціонування мережі.

Застосування технології NAT для забезпечення доступу до Інтернету через провайдера дозволить змінювати внутрішні IP-адреси комп'ютерного клубу під час зовнішнього з'єднання, що підвищує рівень безпеки мережі.

2.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації;

LAN_1 – Технічний сервіс був створений за для забезпечення комунікацій та підтримки технічного обслуговування. У загальному обсязі, ма9 вузлів; підтримка технології EtherChannel для збільшення пропускної здатності та відмовостійкості мережі.

Вимоги до ієрархії: Два рівні ієрархії: LAN_1 і центральний сервер.

Ступінь централізації: Централізоване управління і моніторинг через центральний сервер.

LAN_2 – Головна ігрова зала:

Призначення: Надання доступу до ігрових ресурсів.

Основні характеристики: 68 вузлів; логічне розділення мережі.

LAN_3 – Зовнішня ігрова зала:

Призначення: Мережа для зовнішньої ігрової зони клубу.

Основні характеристики: 116 вузлів;

LAN_4 – Лобі:

Призначення: Мережа для лобі клубу.

Основні характеристики: 122 вузли; використання технології NAT для забезпечення доступу до Інтернету через провайдера. VPN для забезпечення захищеного з'єднання з головною мережею.

LAN_5 – Бухгалтерія:

Призначення: Мережа для бухгалтерського відділу клубу.

Основні характеристики: 58 вузлів; використання VLAN для логічного розділення мережі та забезпечення безпеки даних.

2.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи

Ethernet-кабелі

– VPN для забезпечення захищеного віддаленого доступу;

– Wi-Fi забезпечує можливості бездротового підключення;

– Bluetooth виробнича специфікація бездротових персональних мереж (Wireless personal area network, WPAN). Bluetooth дозволяє цим пристроям повідомлятись, коли вони знаходяться один від одного в радіусі 100м.

2.1.1.3 Вимоги до її сумісності

Використання протоколів обміну даними, таких як HTTP, HTTPS, FTP, TCP/IP, для забезпечення надійної та безпечної комунікації між системами.

Підтримка стандартів API та веб-сервісів (REST, SOAP) для інтеграції з іншими програмами та сервісами.

Програми повинні підтримувати роботу на різних апаратних платформах та бути сумісними з існуючим обладнанням.

Використання протоколів FTP/SFTP для безпечного обміну файлами між системами.

Використання методів шифрування для захисту даних під час їх передачі між системами.

Усі встановленні додадтки, програми, та ПЗ повинні бути сумісними з основними операційними системами (Windows, Linux) та іншими програмними продуктами.

2.1.1.4 Вимоги до режимів функціонування

Основний режим роботи передбачає використання ігрових систем для симуляторів, роботи з браузером та системними програмами. У цьому режимі важливо забезпечити стабільність роботи всіх робочих станцій та серверів. Крім того, слід реалізувати захист від шкідливих програм і атак на рівні мережі та робочих станцій, а також дотримуватися політик безпеки та обмежувати доступ до небажаних ресурсів.

Адміністративний режим використовується адміністраторами для керування системою, внесення змін у налаштування та моніторингу її роботи. У цьому режимі необхідний повний доступ до всіх компонентів системи. Адміністратори повинні мати можливість швидко реагувати на помилки у системі та вирішувати проблеми.

Планове технічне обслуговування включає регулярні роботи з обслуговування і перевірки стану системи.

Аварійне технічне обслуговування передбачає проведення робіт у випадку виявлення серйозних проблем або несправностей. Вимоги до цього режиму включають швидке виявлення та усунення несправностей, наявність резервних компонентів для швидкої заміни та можливість швидкого відновлення працездатності системи.

2.1.1.5 Перспективи розвитку, модернізації Системи

Плани розвитку комп'ютерного клубу "СКАЛА" включають поступове оновлення комп'ютерів для підтримки сучасних ігор та програмного

забезпечення, встановлення швидкісних маршрутизаторів та комутаторів для поліпшення мережевої інфраструктури та зменшення Input lag’у, ping’у тощо, впровадження енергоощадних технологій та обладнання для зменшення витрат на електроенергію, розширення площі клубу та створення нових залів для різних видів діяльності, таких як зали для свого кафе, VR-ігор та окремі зони відпочинку, а також відкриття нових філій клубу в інших містах для розширення мережі та залучення більшої кількості клієнтів.

2.1.1.6 Вимоги до чисельності і кваліфікації персоналу, що обслуговує Систему і режиму його роботи

Адміністратор системи повинен мати вищу освіту в галузі інформаційних технологій, знання мережевих технологій, системного та мережевого адміністрування, а також навички роботи з програмним забезпеченням таким як CyberCafePro. На кожну зміну має бути присутній хочаб один адміністратор

Тех. персонал повинен складатися з кількох технічних спеціалістів з комп’ютерної інженерії.

2.1.1.7 Вимоги до чисельності персоналу (користувачів) Системи

Враховуючи необхідність цілодобового режиму роботи клубу, кожен із персоналу повинен працювати позмінно. Це означає, що загальна чисельність персоналу може складати від 10 до 12. Також треба розуміти, що така підприємство як комп’ютерний клуб не предбачує великого штату працівників, а тому технічний інженер може робити роботу системного інженеру.

2.1.1.8 Вимоги до кваліфікації персоналу, порядку його підготовки і контролю знань і навичок

Щоб підготувати адміністратора котрий зможе виконувати поставленні задачи треба наступне:

– початкове навчання з налаштування та використання CyberCafePro;

– курси з підвищення кваліфікації щодо нових версій програмного забезпечення та сучасних технологій у сфері IT;

– знання мережевих технологій, системного та мережевого адміністрування.

2.1.1.9 Вимоги до надійності

Для ефективної організації мережі комп'ютерного клубу "СКАЛА" з великою кількістю комп'ютерів та складними вимогами до мережі необхідно використовувати комутатори з високою пропускною здатністю та підтримкою VLAN для розділення мережі на сегменти. Кожен VLAN повинен мати свій окремий комутатор для забезпечення безпеки та ефективності мережі. Для забезпечення взаємозв'язку між віддаленими мережами та LAN використовуємо надійні маршрутизатори з підтримкою маршрутизації між VLAN та VPN для безпечного з'єднання мереж. Для ефективного управління та моніторингу мережі використовується спеціальне програмне забезпечення (CyberCafePro) для виявлення проблем та віддаленого керування обладнанням. Мережу треба оснастити захистом, використовуючи файрволи, системи виявлення та запобігання вторгнень та регулярні оновлення програмного забезпечення для запобігання вразливостям.

Вимоги до надійності ігрових периферійних пристроїв, таких як ігрові рулі з педалями, джойстики, контролери для польотних симуляторів та ВР шоломи, включають використання високоякісних матеріалів. Конструкція повинна бути міцною і ергономічною, щоб забезпечити комфорт користувача протягом тривалого користування. Матеріали повинні бути стійкими до зношування і механічних пошкоджень, що дозволить підвищити тривалість служби пристроїв. Додатково, важливо, щоб поверхні були антибактеріальними та неслизькими, щоб забезпечити безпечне користування навіть під час інтенсивного використання.

Приклади матеріалів, які можуть бути корисні для таких пристроїв:

Пластик: Для корпусів і елементів, які повинні бути легкими і міцними.

Метал: Для арматури і осей, що потребують додаткової міцності.

Гума: Для покриття ручок і педалей, щоб забезпечити комфорт і зручність захоплення.

Силікон: Для виготовлення антибактеріальних і неслизьких поверхонь, які зменшують ризик використання.

Треба призначити кілька змін, бо клуб планує працювати цілодобово

Ранкова зміна (8:00-16:00), денна зміна (16:00-00:00), нічна зміна (00:00-8:00).

2.1.1.10 Вимоги безпеки

Забезпечення доступу лише авторизованим працівникам та клієнтам.

Використання фаєрволів, оновлення антивірусного програмного забезпечення.

Захист мережі Wi-Fi в клубі паролем для запобігання несанкціонованому доступу.

Регулярне створення резервних копій даних клієнтів та системних даних.

2.1.1.11 Вимоги до ергономіки та технічної естетики

Всі робочі місця повинні бути обладнані регульованими столами та стільцями для забезпечення комфортної посадки користувачів різного зросту та комплекції.

Екрани моніторів повинні бути розташовані на рівні очей користувача або трохи нижче, щоб зменшити навантаження на шию та очі.

Клавіатура та миша повинні бути розташовані так, щоб руки користувача були в нейтральному положенні, а кут згинання ліктя не перевищував 90 градусів.

Підтримувати комфортну температуру в приміщенні (близько 20-24°C).

Підтримувати відносну вологість повітря на рівні 40-60%.

Забезпечити хорошу вентиляцію приміщення для запобігання перегріву техніки та забезпечення свіжого повітря.

Використовувати матеріали для поглинання шуму, щоб знизити рівень шуму від обладнання та користувачів.

Використовувати сучасне обладнання з естетично привабливим дизайном.

Ретельно організувати кабелі, використовуючи кабель-канали та органайзери для уникнення безладу.

Зони відпочинку:

– обладнати зони відпочинку м'якими меблями та розважальними засобами для комфортного відпочинку користувачів між сесіями роботи за комп'ютером;

– використовувати декоративні рослини для покращення атмосфери та створення більш приємного середовища.

2.1.1.12 Умови і регламент (режим) експлуатації

Для забезпечення надійної експлуатації технічних засобів у комп'ютерному клубі необхідно визначити регламент експлуатації, що забезпечать використання обладнання з заданими технічними показниками. Ось аспекти, які потрібно врахувати:

а) Мікро климат.

Оптимальна робоча температура у приміщенні клубу повинна знаходитися в діапазоні від 18°C до 24°C. Температура з 18°C до 24°C є комфортною для людей. В такому середовищі користувачі можуть довше залишатися в клубі без відчуття дискомфорту також не треба забувати що у оптимальному температурному діапазоні, системи охолодження та вентиляції працюють більш ефективно, що знижує загальне енергоспоживання клубу.
Максимально допустимі температурні відхилення: від 15°C до 30°C.

б) Вологість.

Оптимальна відносна вологість повітря: 40-60%.

Максимально допустима вологість: 30-70%.

Все це допомагає зменшити накопичення статичної електрики, яка може пошкодити електронні компоненти комп'ютерів та іншого обладнання.

в) Пил і забруднення.

Регулярне прибирання та очищення приміщень від пилу і бруду у спеціально обрані дні неділі.

Пил може потрапляти всередину комп'ютерів та іншого обладнання, що може призвести до перегріву, зниження продуктивності та навіть пошкодження комплектуючих. Накоплений пил у вентиляційних отворах та фільтрах, зменшує ефективність охолодження, що впливати на стабільність роботи обладнання.

г) Вентиляція та охолодження:

Наявність ефективної системи вентиляції та кондиціонування для запобігання перегріву обладнання.

Перевірка справності вентиляційної системи потрібно перевіряти не менше одного разу на тиждень, за для уникнення не передбачанних проблем.

д) Види обслуговування:

Профілактичне обслуговування: Чистка, Перевірка з'єднань, оновлення програмного забезпечення, перевірка та тестування обладнання, архівування та резервне копіювання

Коригувальне обслуговування: Заміна зламаних або зношених компонентів, таких як жорсткі диски, оперативна пам'ять, графічні карти, блоки живлення, контролери тощо.

Перевірка та повторне підключення або заміна несправних кабелів, контролерів і роз'ємів.

Аварійне обслуговування: оперативні дії у разі виникнення непередбачуваних поломок або збоїв у роботі.

Швидка заміна або ремонт несправних компонентів (жорстких дисків, оперативної пам'яті, графічних карт, блоків живлення тощо).

Використання резервних копій для відновлення втрачених або

пошкоджених даних. Перевірка і відновлення підключення до інтернету, включаючи налаштування маршрутизаторів і комутаторів.

За можливості, пропонування клієнтам альтернативних робочих місць або відшкодування за час простою.

2.1.1.13 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

Склад повинен бути розташований в місці де немає доступу для сторонніх осіб.

Зберігання запасних виробів і приладів повинно здійснюватися в сухому і прохолодному приміщенні з температурою в межах 18-24°C та відносною вологістю 40-60%.

Шкаф серверний Estap EVL70126U6010L34M50, чорного кольору, має такі характеристики:

Висота: 26U (приблизно 1146 мм)

Глибина: 1000 мм

Двері: перфоровані

Для зберігання серверного обладнання, забезпечуючи відмінну вентиляцію та доступ до обладнання.

2.1.2.6 Вимоги до захисту інформації від несанкціонованого доступу;

Антивірусне програмне забезпечення:

Важливо періодично оновлювати базу даних вірусних сигнатур та програмне забезпечення самого антивірусу для забезпечення ефективного захисту від нових загроз.

Фаєрвол:

Фаєрвол має бути налаштований на фільтрацію вхідного та вихідного трафіку.

Обмеження доступу до певних портів, протоколів та IP-адрес, які не є

необхідними для роботи комп'ютерного клубу.

Контроль доступу:

Налаштування аутентифікації користувачів:

Встановлення паролів на всі мережеві пристрої (маршрутизатори, комутатори).

Налаштування локальних облікових записів з різними рівнями привілеїв.

Використання ACL (Access Control Lists):

Створення та застосування списків контролю доступу (ACL) для обмеження доступу до мережевих ресурсів.

Налаштування ACL на інтерфейсах маршрутизаторів та комутаторів для фільтрації вхідного та вихідного трафіку.

Конфігурація VTY ліній:

Налаштування VTY (Virtual Teletype) ліній для обмеження доступу до мережевих пристроїв через SSH.

Використання ACL для обмеження доступу до VTY ліній тільки з певних IP-адрес.

SSH доступ:

Налаштування SSH для безпечного віддаленого доступу до мережевих пристроїв.

Моніторинг та аудит доступу:

Налаштування систем журналювання на мережевих пристроях для запису спроб доступу.

Регулярний перегляд журналів для виявлення підозрілої активності.

Оновлення програмного забезпечення:

Регулярне оновлення програмного забезпечення є необхідною умовою для забезпечення безпеки та стабільної роботи комп’ютерного клубу. Це допоможе запобігти використанню вразливостей, які можуть призвести до несанкціонованого доступу, крадіжки даних або інших проблем.

Треба активувати автоматичні оновлення для операційних систем,

антивірусного ПЗ та іншого критично важливого ПЗ.

Регулярне проведення перевірки наявності нових оновлень для всього програмного забезпечення, встановленого на комп’ютерах. Включаючи оновлення обладнення від NVIDIA, AMD.

Забезпечити можливості швидкого відкату до попередньої версії програмного забезпечення у разі проблем з оновленням.

2.1.1.14 Вимоги до схоронності інформації при аваріях

Для забезпечення схоронності інформації при аваріях необхідно впровадити регулярне резервне копіювання та відновлення даних, фізичний та кіберзахист обладнання. Створення локальних бібліотек на серверах, таких як TFTP, забезпечує захист інформації шляхом регулярного резервного копіювання даних. Це також забезпечує можливість швидкого відновлення в разі втрати даних завдяки наявності збережених копій конфігурацій та інших важливих файлів.

2.1.1.15 Вимоги до радіоелектронного захисту засобів

Захист від електромагнітних завад (ЕМЗ)

Використання екранірованих кабелів для передачі даних та живлення для зменшення впливу електромагнітних завад.

Екранування приміщень:

Встановлення екрануючих матеріалів(Полімерні композити) у стінах, підлогах та стелях приміщень для захисту від зовнішніх електромагнітних випромінювань.

Встановлення фільтрів електромагнітних завад (EMI) на електропроводку та інші комунікації для запобігання проникненню завад у систему.

Використання захищених протоколів (WPA3) для шифрування трафіку в бездротових мережах.

2.1.1.16 Вимоги до патентної чистоти

Патент використовується на території України.

2.1.1.17 Вимоги до стандартизації й уніфікації

Забезпечення відповідності розроблюваних продуктів та технологій державним, галузевим і міжнародним стандартам.

Використання стандартів ISO, IEC, ДСТУ та інших, релевантних до конкретної галузі.

IEC 60950-1 та IEC 62368-1

для забезпечення безпеки обладнання та захисту користувачів від потенційних ризиків.

ISO 9001:2015

Стандарти управління якістю. Забезпечує структуру для управління якістю продуктів і послуг, включаючи управління процесами, ресурсами, аналіз результатів та постійне вдосконалення.

IEC 62368-1:2018

Стандарти безпеки аудіо/відео, інформаційно-комунікаційного і технологічного обладнання. Включає вимоги до конструкції і виготовлення обладнання для забезпечення його безпечного використання.

ДСТУ Б В.2.7-19-95

Вимоги до матеріалів і конструкцій будівельних об’єктів, які можуть використовуватися в облаштуванні приміщень комп'ютерного клубу.

ISO 14721:2012

Системи управління цифровими об'єктами інформації. Загальні вимоги містить вказівки щодо зберігання електронних даних та обладнання.

2.1.1.18 Функцій (задач) Системи і програмних засобів, що поставляються

Моделювання мережі:

Створення та візуалізація мережевої топології.

Підтримка різних типів мережевих пристроїв (маршрутизатори, комутатори, комп'ютери, сервери тощо).

Моделювання різних мережевих технологій (LAN).

Конфігурація пристроїв:

Налаштування мережевих параметрів пристроїв (IP-адресація, маршрутизація, VLAN, NAT).

Використання командного рядка (CLI) для конфігурації пристроїв Cisco.

Підтримка симуляції командних інтерфейсів для налаштування пристроїв.

Тестування та налагодження:

Використання інструментів для перевірки з'єднань та діагностики мережевих проблем.

Можливість запуску пакетних трасувань (Packet Tracing) для аналізу руху даних у мережі.

Використання засобів моніторингу та аналізу для виявлення та усунення помилок.

Віртуалізація мережевих сценаріїв:

Створення різних сценаріїв для навчання та тестування мережевих концепцій.

Використання сценаріїв для імітації реальних умов роботи мережі.

Підтримка багаторазового використання сценаріїв для навчальних цілей..

Оновлення програмного забезпечення має здійснюватися регулярно для забезпечення актуальності функцій та безпеки. Технічна документація на Cisco Packet Tracer повинна бути повністю описана, включаючи інструкції з встановлення, налаштування та експлуатації програмного забезпечення.

2.2 Типових проектних рішень;

Кількість ігрових станцій: 40

Характеристики:

Процесор: Ryzen 5 5600X ефективно впоратиметься з вимогливими завданнями VR, такими як симулятори політів, і забезпечити користувачам високу якість графіки та плавну роботу програм, має 6 ядер і 12 потоків, що забезпечує високу швидкодію при обробці багатьох завдань одночасно, що важливо для симуляторів політів і VR-додатків.

Материнська плата: MSI B550-A PRO - Ця плата має хороші відгуки за свої можливості розгону, стабільність і кількість роз'ємів для підключення пристроїв.

Оперативна пам'ять: Corsair Vengeance LPX 16GB (2 x 8GB) DDR4-3200 - це достатньо пам'яті для більшості завдань.

Жорсткий диск: Seagate Barracuda 2TB 7200RPM - це надійний жорсткий диск з великою ємністю для зберігання даних.

SSD: Kingston A2000 500GB NVMe PCIe M.2 - це швидкий SSD для операційної системи та програм.

Відеокарта: NVIDIA GeForce RTX 3060 - ця відеокарта можуть запускати сучасні ігри та обробляти відео. Підтримує технологію відслідковування променів (Ray Tracing), що дозволяє досягати більш реалістичного освітлення і візуальних ефектів у сучасних іграх і VR-додатках.

Блок живлення: EVGA SuperNOVA 650 G5, 80 Plus Gold 650W - цей блок живлення надійно живить нашу систему.

Корпус: NZXT H510 або Fractal Design Meshify C - ці корпуси мають хорошу вентиляцію та зручний дизайн.

Монітор: ASUS TUF Gaming VG27AQ - цей монітор з високою якістю зображення та частотою оновлення.

Миша: Logitech G502 HERO та Клавиатура: Corsair K55 RGB Pro (CH-9226765-NA) - це якісні та зручні пристрої для введення даних.

Маршрутизатори:

Cisco UCS C240 M5 Server: Маршрутизатор має високу продуктивність та включає в себе контролер UniFi для керування мережею.

Cisco 2911 Integrated Services Router: Маршрутизатор підтримує швидкість передачі даних до 900 Мбіт/с та має низький рівень споживання енергії.

Комутатори:

Cisco Catalyst 2960-24TT: Комутатор має високу швидкість передачі даних і підтримує кілька портів Gigabit Ethernet для підключення комп'ютерів і пристроїв.

Комутатор підтримує швидкість передачі даних до 1 Гбіт/с на кожном порту і має надійну роботу.

Ігрові периферійні пристрої:

Проводной руль Logitech G29 Driving Force: відчуття керування зближене до реального автомобіля, що дозволяє користувачам максимально відчувати грі відеоігор з автомобільними симуляторами.

Окуляри-шолом віртуальної реальності SHINECON VR SC-G02ED:
вони мають зручну конструкцію і можуть бути зручними для тривалого використання, що важливо для іммерсивного VR-досвіду.

Проводной джойстик Logitech X-56 Rhino Saitek Pro Flight (945-000059):
наближена до реального відчуття керування літаком, що додає іммерсивності ігровому досвіду.

2.2.1 Вимоги до використання типових компонентів і комплексів

Сумісність:

Всі компоненти повинні бути сумісними між собою та працювати стабільно в мережевому середовищі клубу. (йдеться про сумісності компонентів ігрових станцій таких як материнська плата, відео адаптери та процесори. Вони повинні працювати в одній тактовий частоті)

Програмне забезпечення повинно бути сумісне з операційною системою та іншими програмами, що використовуються в клубі.

Ергономіка:

Робоче місце повинно бути організоване з урахуванням зручності для користувача. Тобто, люди які використовують контролери для симуляції повинні знаходитись на відстані витягнутої руки зазвичай це 60-70 сантиметрів.

Монітори повинні бути розташовані на відстані, яка не перевищує оптимальний параметр для запобігання втомі очей. (рекомендується в діапазоні від 50 до 70 сантиметрів)

Характеристики обладнання:

Комп'ютери повинні мати достатню продуктивність для виконання завдань клубу.

Оперативна пам'ять (RAM): від 16 гігабайт. Це дозволяє запускати сучасні ігри та багатозадачні програми без проблем.

Відеокарта (GPU): Від 6 гігабайт відеопам'яті, щоб забезпечити високу продуктивність графіки в іграх.

Процесор (CPU): Частота від 3,5 до 5,0 гігагерц.

Накопичувач (Storage): SSD обсягом від 500 гігабайт до 1 терабайт для швидкого завантаження ігор і швидкого доступу до даних.

Монітори повинні мати високоякісне зображення, яке забезпечує чіткість, насиченість кольорів, високу роздільну здатність і при цьому мінімальний рівень мерехтіння. В нашому випадку використовуємо IPS (In-Plane Switching) IPS матриці мають кращі кольори і ширший кут огляду, що робить їх ідеальними для професійної графіки та кольорової точності. Вони забезпечують кращу рівномірність яскравості по всьому екрану.

Клавіатури та миші повинні бути зручними для користування та мають бути з високоякісного пластика та гарним ПЗ. (підтримка програмного забезпечення для налаштування клавіш і підсвічування та преміальні механічні перемикачі для високої швидкодії та комфорту.)

2.2.2 Додаткові вимоги

Мережева безпека: Налаштування брандмауерів, VPN, мережевих політик

безпеки для захисту мережі від несанкціонованого доступу та зовнішніх загроз.

Моніторинг та аналіз мережі IoT: Встановлення системи моніторингу мережі у планшетні ПК , за для аналізу трафіку та ефективності мережі.

Безпека даних: Резервне копіювання даних у локальних бібліотеках

Керування мережею: Забезпечення простого та ефективного керування мережею через віддалений доступ та моніторинг з любого комп`ютера адміністратора.

Оновлення та підтримка: Регулярне оновлення програмного забезпечення та обладнання для запобігання вразливостям та забезпечення найновіших функцій.

2.2.2.1 Вимоги до Системи, пов'язані з особливими умовами її експлуатації;

Простір і вентиляція забезпечу достатній простір для комфортного користування VR шоломом без перешкод. Забезпечу вентиляцію, щоб уникнути перегріву обладнання та дискомфорту для користувача.

2.2.2.2 Вимоги до активного обладнання (функціонування, кількість портів та їх запас, варіанти встановлення, технічні вимоги);

Функціональні вимоги:

Маршрутизація трафіку для забезпечення доступу до Інтернету та інших мережних ресурсів.

Керування мережевим трафіком та безпекою.

Віртуальні приватні мережі (VPN) для забезпечення безпеки під час з'єднання з віддаленими ресурсами.

Управління якістю обслуговування (QoS) для підтримки вимог до швидкодії для різних типів трафіку.

Кількість портів та їх запас:

Для того щоб комп’ютерний клуб працював без проблем, треба встановити комутатори з не менше ніж 24 портами для підключення кожного комп'ютера.

Також не треба забувати що за для розширення треба мати більший запас портів.

Варіанти встановлення:

Монтаж робимо на настінної та стельової установки для оптимального розміщення обладнання у приміщенні комп'ютерного клубу.

Технічні вимоги:

Підтримка Gigabit Ethernet для швидкісного передавання даних між комп'ютерами та мережевим обладнанням.

2.2.2.7 Вимоги до кабель-каналів, інформаційним та електричним розеткам (тип, розмір, варіант розміщення);

Кабель-канали:

Для комп'ютерного клубу використовуваємо металеві та пластикові кабель-канали, це дозволить забезпечити належний рівень безпеки та ефективно організувати монтаж і підключення кабелів у приміщенні клубу.

Розмір: Використання кабель-каналів широкістю від 50 мм до 300 мм, залежно від обсягу кабелів, які потрібно прокласти. Точний розмір кабель-каналів краще визначати після оцінки потреб інсталяції і консультації з фахівцями з монтажу кабельних систем.

Варіант розміщення: Кабель-канали повинні бути легкодоступними для обслуговування та можливого ремонту.

Електричні розетки:

Тип: Стандартні розетки для електрики та мережі. Металеві або високоякісні пластикові корпуси, які мають відповідати стандартам пожежної безпеки і мають високу механічну міцність. Металеві корпуси або високоякісний пластик забезпечують відмінну захист від фізичних пошкоджень, які можуть виникнути

внаслідок ударів або неправильного використання. Ці матеріали мають високу температурну стійкість і важливі для забезпечення безпечності у разі виникнення короткого замикання чи інших електричних проблем.
Розмір: Відповідно до можливості розміщення розеток у приміщеннях.
Варіант розміщення: Розташовуємо близько до робочих с
толів для живлення комп'ютерів, моніторів та інших електронних пристроїв.

2.2.2.8 Вимоги до комунікаційного обладнання і його розташування (розташування у приміщенні, тип шаф, тип підводу кабельних трас, розташування обладнання усередені шафи);

Розташування у приміщенні:

Комунікаційне обладнання повинно бути розташоване в зручному для доступу місці, щоб забезпечити легкий доступ для технічного обслуговування і відладки.

Тип шаф:

Використання стійок або шаф для монтажу комунікаційного обладнання, таких як стійки 19 дюймів, що відповідають стандартам для монтажу серверного обладнання і комутаційних пристроїв. Шафа для кабелів 19 дюймів є стандартом у багатьох системах комунікаційного обладнання і серверних приміщеннях. Вона призначена для монтажу різноманітного обладнання, яке відповідає цьому стандарту, такого як комутатори, маршрутизатори, сервери.

Основні характеристики 19-дюймової шафи включають:

Висота: зазвичай стандартна висота шафи може бути 42U (приблизно 2 метри) або 24U (близько 1.2 метра), хоча можливі і інші варіанти.

Глибина: 100 см, що забезпечує достатньо місця для установки обладнання та забезпечення теплообміну.

Ширина: стандартна ширина шафи для кабелів 19 дюймів (близько 48 см), що відповідає стандартним ширинам обладнання.

Використовування кабельних каналів та лотків для організації кабельних трас, що забезпечує безпеку кабелів і легкість доступу для підключення і заміни.

Розташування обладнання усередині шафи:

Обладнання монтується на спеціальній рамі (рейці), яка забезпечує кріплення різних пристроїв. Рейки можуть бути регульовані по висоті, щоб адаптуватися під розміри конкретного обладнання. Ці пристрої можуть будуть розміщені в нижній частині шафи, де є достатньо місця для їхнього розташування і забезпечення необхідного теплообміну. До шафи встановлюваємо інші пристрої, такі як сервери, мережеві адаптери.

2.2.2.9 Вимоги до однорідності (тип кабелів, роз’ємів, магістралей т.ін.);

Кабелі Ethernet: Використання високоякісних кабелів Ethernet, які відповідають стандартам категорій 6. використання UTP (Unshielded Twisted Pair) кабелів для легкої установки і мінімізації електромагнітних перешкод.

Роз'єми RJ-45: Використання стандартних роз'ємів RJ-45 для підключення комп'ютерів, принтерів і іншого обладнання до мережі.

Магістралі Ethernet: Використання магістралей Ethernet для підключення комутаторів і маршрутизаторів у мережі. Використання оптоволоконних кабелів для великих відстаней або до високої швидкості передачі даних.

Для спеціалізованих підключень можна використовувати інші типи кабелів, такі як USB, HDMI, DisplayPort.

2.2.2.10 Вимоги до розширюваності

Резервні порти: Додаткові порти на комутаторах і маршрутизаторах для можливості підключення нового обладнання без необхідності заміни основного обладнання.

Резервні мережеві шнури: Додаткові мережеві кабелі для підключення нових пристроїв або для заміни пошкоджених кабелів.

Масштабованість комутаторів і маршрутизаторів: Використання комутаторів і маршрутизаторів, які підтримують додаткові модулі для розширення кількості портів або функціональності.

Масштабованість мережевого обладнання: Використання мережевого обладнання, яке підтримує класифікацію трафіку, віртуальні мережі (VLAN) та інші технології для ефективного управління мережею при збільшенні кількості підключених пристроїв.

Резервні блоки живлення: Наявність резервних блоків живлення для обладнання для уникнення відмов у разі відмови основного блока живлення.

Резервні ігрові периферійні пристрої: Наявність резервних пристроїв, які можуть бути швидко підключені у випадку виходу основного пристрою з ладу.

2.2.2.12.1 Вимоги до резервування

Регулярне створення резервних копій даних і зберігання їх на окремих носіях або в хмарних сховищах для запобігання втраті важливої інформації.

Не треба забувати про наявність додаткових компонентів (комп'ютерів, моніторів, клавіатур, мишей) для заміни пошкоджених або відмовних пристроїв.

Наявність додаткового обладнання (мережевих комутаторів, маршрутизаторів) для заміни основного обладнання у разі відмови, теж передбачаються.

2.2.2.12Спеціальні вимоги

Підтримка протоколів IoT: Забезпечення сумісності з протоколами IoT, такими як MQTT, HTTP, для забезпечення взаємодії з IoT-пристроями.

Інтеграція з IoT-пристроями: Можливість підключення до різних типів IoT-пристроїв (датчики, контролери, пристрої збору даних) для моніторингу та управління ними.

Безпека IoT: Захист IoT-пристроїв та даних, що передаються, за допомогою шифрування, аутентифікації та авторизації.

Не треба забувати про можливість Tablet-PC збирати та аналізувати потік даних, що надходять від IoT-пристроїв, для отримання інформації про стан IoT-пристроїв. (Рисунок − 2.5)

Рисунок 2.4 – Tablet PC

Можливість інтеграції з іншими системами, є найголовнішою задачою у комп'ютерному клубі, бо треба впровадити такі IoT-пристрої щоб доповнювали та автоматизовували рутинні справи.

Тобто, треба впровадити здатність системи працювати ефективно з великою кількістю IoT-пристроїв та об'ємом даних. Без шкоди для корпоротивної мережі.

Можливість моніторингу стану IoT-пристроїв та віддаленого керування ними через циско покет трейсер, буде гарною ідеєю бо це дуже легко, та маємо можливість перевіряти различні ситуації у тестовому просторі щоб перевірити роботоспособність нашої системи.

2.3 Вимоги до функцій (задач), виконуваним Системою

Постійний моніторинг роботи комп'ютерів для виявлення можливих проблем або відмов. Оптимальне розподілення ресурсів (часу використання, мережевої пропускної здатності) між користувачами.

Збір та аналіз даних про використання комп'ютерів для підвищення ефективності роботи клубу.

Регулярне оновлення програмного забезпечення на комп'ютерах та управління цим процесом.

Адміністрування користувачів є можливісттю управління реєстрацією, правами доступу та іншими аспектами користувацьких облікових записів.

Розширені можливості: інтеграція з VR платформами та додатками, забезпечення стабільної роботи VR шоломів та контролерів.

2.3.1 Вимоги до налаштувань та функцій, які виконує Система

Щоб киберфізична система працювала, необходно зробити наступні кроки:

1. Наявність свободного порту (USB) та простору для підключення

2. Оновити драйвера для контролерів та шоломів VR (Треба розуміти що такі VR-шоломи як Oculus, не можуть працювати без офіційних ПЗ)

3. Налаштування кожен користувач робить під себе. В кожному конкретному симуляторі є спеціальні категорії.

Щоб корпоротивна мережа працювала, необхідно здійснити наступні кроки за для налаштування маршрутизаторів та комутаторів:

1. Призначємо унікальні імена кожному пристрою, дотримуючись формату Sorocopud_тип пристрою_номер пристрою, і налаштуйте банер MOTD, який включає доменне ім'я, ідентичне імені цього пристрою.

2. Встановлюємо пароль "cisco" для консольних та vty ліній на всіх пристроях, і пароль "class" для доступу до привілейованого режиму. Забезпечте, щоб ці паролі зберігалися у зашифрованому вигляді за допомогою RSA-ключа довжиною 1024 біти.

3. Встановлюємо використання протоколу SSH на всіх vty лініях.

4. Створюємо користувача з найменуванням 123201_Sorocopud і паролем admin на всіх пристроях.

5. Щоб DCE-інтерфейс запрацював як нам треба, встановлючаємо частоту маршрутизаторів 128000;

6. Пропускна спроможність serial, дорівнює 128 Кб/с;

7. Призначити адреса маршрутизаторів;

8. Виконуємо налаштування протоколу RIP, вказавши мережі, що підключені до нього.

9. На граничних маршрутизаторах встановити статичні маршрути мережі Internet і мережі провайдера.

10. На всіх маршрутизаторах налаштувати підтримку служби AAA з використанням локальної бази даних користувачів для доступу до vty ліній та протоколу RADIUS для консольного доступу. Налаштувати RADIUS-сервер так, щоб для автентифікації користувачів використовувалися імена пристроїв та пароль admin123, а ключове слово було radius123.

11. Забезпечити безпеку інформації у системі за допомогою налаштування VLAN на маршрутизаторі, що призначений для адміністративного та управлінського персоналу.

12. Налаштувати безпеку портів на комутаторах, які з'єднані з серверами таким чином, щоб доступ до портів мали лише два унікальні пристрої, з динамічним розпізнаванням їх MAC-адрес.

Функції, що повинна виконувати Система:

1. Забезпечення надійного, оперативного та швидкого зв'язку між користувачами комп'ютерної системи клубу.

2. Забезпечення можливості безпечного з'єднання користувачів з мережею Інтернет, отримання і обміну інформацією між ними.

3. Забезпечення збереження та резервного копіювання інформації на серверах, а також захист від зовнішніх та внутрішніх загроз.

4. Захист компонентів системи від зовнішніх втручань та вірусів.

5. Забезпечення зашифрування IP-адрес пристроїв.

6. Обмеження доступу до пристроїв комп'ютерної системи зі сторонніх вузлів.

7. Розділення підмереж підприємства на відділи, у разі необхідності,для

сегментування праці, ПЗ, тощо;

8. Ігрова станція повинна автоматично виявляти підключені пристрої та інформувати користувача про їх готовність до використання.

Щоб працювали усі системи IoT треба зробити наступне:

1. Підключаємо IoT пристрої до пІдмережі.

2. Налаштовуваємо параметри кожного пристрою, такі як IP-адреси, мережеві налаштування і специфічні конфігурації.

3. Налаштовуємо маршрутизатори і комутатори для забезпечення зв'язності в мережі. Вказуємо VLAN, налаштування маршрутизації і інші параметри мережі.

4. Моніторинг і управління нашою IoT мережею буде забеспечувати TabletPC.

2.3.2 Часовий регламент і вимоги одночасності виконання групи функцій, вірогідності видачі результатів

Часовий регламент: Постійний доступ з обмеженням часу користування (Не більше чим куплений тариф).

Форма представлення: Графічний інтерфейс користувача з доступом до списку ігор. (Забезпечується через спеціальне ПЗ таке як CyberCafePro)

Точність і час виконання: Завантаження гри не більш ніж 30 секунд, без помилок.

Одночасність виконання: Можливість доступу до декількох ігор для різних користувачів.

Вірогідність результатів: 99% успішного запуску ігор без збоїв.

Інтернет-браузер

Постійний доступ з фільтрацією шкідливих сайтів. Повинна забезпечувати високу швидкість завантаження сторінок та фільтрація небезпечного контенту.

Завантаження сторінок не більше 5 секунд, точність фільтрації − 95%. З підтримкою багатозадачності в браузері.

Вірогідність результатів: 98% безпечного перегляду веб-сторінок.

Обслуговування системи

Планове обслуговування раз на тиждень з формою представлення (звіти) про виконання технічних робіт. Не більше 2 годин з початку тех.робіт.

Вірогідність результатів: 99.5% успішного завершення обслуговування.

Моніторинг і звітність

Регулярне оновлення даних (раз на добу) повинні мати точні звіти про стан системи.

2.3.3 Перелік і критерії відмов, по якій задаються вимоги до надійності.

Маршрутизація трафіку:

Відмова: Втрата зв'язку між мережевими сегментами.

Критерії відмови: Переривання підключення до інтернету, відсутність можливості передачі даних між комп'ютерами в мережі.

Безпека мережі:

Відмова: Несанкціонований доступ до мережевих ресурсів.

Критерії відмови: Наявність вторгнень в мережу, втрата конфіденційності або цілісності даних.

Моніторинг мережі:

Відмова: Втрата можливості відстеження стану мережі.

Критерії відмови: Невідповідність вимогам до частоти збору статистики, помилки в аналізі даних.

Резервне копіювання даних:

Відмова: Втрата або пошкодження архівованих даних.

Критерії відмови: Недостатня кількість резервних копій, відсутність можливості відновлення даних.

Обслуговування та технічна підтримка:

Відмова: Несправність системи підтримки користувачів.

Критерії відмови: Незадовільний час реакції на звернення користувачів, недоступність необхідного обладнання або програмного забезпечення для вирішення проблем.

високу продуктивність для роботи та ігор.

Материнські плати: MSI B550-A PRO S, які мають достатню кількість портів для підключення компонентів.

Оперативна пам'ять: Corsair Vengeance LPX 16GB (2 x 8GB) DDR4-3200 для забезпечення високої швидкості та ефективності роботи.

Жорсткі диски: Seagate Barracuda 2TB 7200RPM для зберігання великих обсягів даних.

SSD: Kingston A2000 500GB NVMe PCIe M.2 для швидкого завантаження операційної системи та програм.

Відеокарти: NVIDIA GeForce RTX 3060 для запуску сучасних ігор та обробки графіки.

Блоки живлення: EVGA SuperNOVA 650 G5, 80 Plus Gold 650W для стабільного живлення всієї системи.

Корпуси: NZXT H510 або Fractal Design Meshify C з хорошою вентиляцією та зручним дизайном.

Монітори: ASUS TUF Gaming VG27AQ або LG 27GL850-B для високоякісного зображення та високої частоти оновлення.

Клавіатури та миші: Logitech G502 HERO та Corsair K55 RGB для зручності та точності введення даних.

Ігрові периферійні пристрої:

Проводной руль Logitech G29 Driving Force PC, Окуляри-шолом віртуальної реальності SHINECON VR SC-G02ED, Проводной джойстик Logitech X-56 Rhino Saitek Pro Flight (945-000059) − всі ці контролери забезпечують роботоздатності нашої кіберфізичної системи.

Мережеве обладнання:

Маршрутизатори: Ubiquiti UniFi Dream Machine (UDM) для високої продуктивності та керування мережею або Cisco RV340, що підтримує швидкість передачі даних до 900 Мбіт/с.

Комутатори: Cisco Catalyst 2960-L для високошвидкісної передачі даних та NETGEAR ProSAFE GS108 для надійної роботи.

Wi-Fi точки доступу: Ubiquiti UniFi AP для високошвидкісної передачі даних та NETGEAR Nighthawk AX12, що підтримує стандарт Wi-Fi 6.

Програмне забезпечення:

Операційна система: Ліцензійні версії операційних систем (наприклад, Windows 10 або 11), які забезпечують стабільну та безпечну роботу.

Антивірусне програмне забезпечення: Ліцензійні антивірусні програми для захисту від шкідливого ПЗ.

2.3.4 Вимоги до точності вимірів параметрів

Температура:

Точність вимірювання температури в приміщенні повинна бути не гірше ±0.5°C для забезпечення оптимальних умов експлуатації обладнання.

Вологість:

Точність вимірювання відносної вологості повітря повинна бути не гірше ±3% RH для підтримки необхідних кліматичних умов.

Електрична напруга:

Точність вимірювання напруги електричної мережі повинна бути не гірше ±1% для забезпечення стабільної роботи обладнання.

Пропускна здатність мережі:

Точність вимірювання швидкості передачі даних в мережі повинна бути не гірше ±5% для моніторингу продуктивності і забезпечення якості обслуговування.

Затримка в мережі:

Точність вимірювання затримки (latency) повинна бути не гірше ±5 мс для забезпечення оптимальної роботи мережевих додатків.

2.3.5 Метрологічні характеристики вимірювальних каналів:

Частота калібрування:

Всі вимірювальні прилади повинні калібруватися не рідше одного разу на рік або відповідно до рекомендацій виробника.

Відповідність стандартам:

Вимірювальні прилади повинні відповідати національним і міжнародним стандартам (ДСТУ, ISO, IEC які були наведанні вищче).

2.3.6 Вид метрологічної атестації (державна чи відомча) із указівкою порядку її виконання й організацій, що проводять атестацію.

Державні органи метрології та стандартизації, такі як Державна служба України з питань праці, Державна служба України з питань захисту прав споживачів, Український державний центр стандартизації, метрології та сертифікації .

Порядок виконання:

1. Подача заявки до відомчого метрологічного підрозділу для проведення метрологічної атестації.

2. Надання необхідної документації та технічних характеристик до відомчого підрозділу.

3. Проведення відомчим підрозділом відповідних перевірок та випробувань обладнання.

4. Після успішного завершення атестації видається свідоцтво про відомчу метрологічну атестацію.

2.4.6 До структури і функцій підрозділів, що беруть участь у функціонуванні Системи чи забезпечують її експлуатацію

Структура і функції підрозділів, що беруть участь у функціонуванні Системи та забезпечують її експлуатацію, повинні бути чітко визначені для забезпечення ефективної роботи. Використання Cisco Packet Tracer дозволяє мережевим інженерам моделювати та тестувати рішення, підвищуючи ефективність і надійність мережевої інфраструктури.

Адміністратор системи:

Управління обліковими записами користувачів.

Налаштування та підтримка системи безпеки.

Регулярне оновлення програмного забезпечення.

Мережевий інженер:

Проектування та впровадження мережевої інфраструктури.

Моніторинг та усунення несправностей мережі.

Використання Cisco Packet Tracer для моделювання та тестування мережевих рішень.

2.4 Апаратного забезпечення комп’ютерного клубу

Для успішної розробки апаратної частини комп'ютерного клубу необхідно ретельно підбирати і компонувати основні компоненти обладнання. Це забезпечить високу продуктивність, надійність і відповідність потребам користувачів клубу.

Розроблена підсистеми яка буде представлена нижче була створена за для оптимизування трафику підприємства:

– головний ігровий зал (LAN_1)

– зовнішний ігровий зал (LAN_2);

– адміністраторська (LAN_3);

– технічний відділ (LAN_4);

– тех. Підтримка (LAN_5)

Всі перелічені підсистеми взаємодіють між собою та утворюють єдину систему підприємства, яка в свою чергу забезпечує потреби персоналу та звичайних користувачив.

Враховуючи можливість перегрузки системи, треба розрахувати максимальну можливу завантаженність системи (яку ми розрахуємо у наступних розділах).

2.5 Розробка загально структури комп’ютерно системи

1. Головний сервер (Dell PowerEdge T340): Обраний через високу продуктивність процесора Cisco UCS C220 M5 Server та достатню пам'ять для обробки даних і запуску віртуальних середовищ.

2. Сервер баз даних (Cisco UCS C220 M5 Server): Велика обсяг пам'яті та висока продуктивність процесора Intel Xeon E-2276M для швидкого доступу до даних та оптимізації роботи з базами даних.

3. Файловий сервер (Cisco UCS C220 M5 Server): Великий обсяг пам'яті для зберігання файлів і резервних копій, надійна робота та просте управління.

4. Сервер аутентифікації (Lenovo ThinkSystem ST50): Швидкий процесор та SSD для ефективного управління доступом користувачів.

5. Комутатори (Cisco Catalyst 2960X-48TS-L): Велика кількість портів для підключення робочих станцій та іншого обладнання, підтримка управління L2/L3 для оптимізації мережевого трафіку.

6. Маршрутизатор (Cisco 2911 Integrated Services Router): Підтримка VPN для безпечного доступу до мережі, два порти WAN для резервування зв'язку.

7. Бездротові точки доступу (Cisco Aironet 3700 Series): Підтримка стандарту 802.11ac та технології MU-MIMO для надійного та швидкого бездротового з'єднання.

8. Ігрові станції (ASUS ROG Strix): Висока продуктивність процесора та потужна відеокарта для запуска сучасних ігор.

9. Адміністративні станції (Dell OptiPlex 7070): Потужний процесор та

достатній обсяг пам'яті для виконання адміністративних завдань.

10. Системні станції (HP EliteDesk 800 G5): Ефективний процесор та SSD для проведення технічного обслуговування обладнання.

11. Мережевий файрвол (Cisco ASA 5506-X): Захист від зовнішніх загроз та моніторинг мережевого трафіку.

12. Система виявлення та запобігання вторгненням (Cisco Firepower 1010): IPS/IDS для виявлення та блокування шкідливих атак у мережі.

13. Модуль керування: Забезпечує керування інфраструктурою клубу, включаючи бездротові точки доступу, комутатори та інше обладнання.

14. LAN, WAN кабелі: Використовується для підключення мережевого обладнання та забезпечення швидкого та стабільного з'єднання.

15. Провідний джойстик: У комбінації з VR-гарнітурами, провідні джойстики можуть забезпечувати більш точне та стабільне керування, особливо в іграх та додатках, де важлива висока точність і мінімальна затримка.

16. Провідний руль: У комбінації з VR-гарнітурами, провідні керма можуть забезпечувати більш точне та реалістичне керування віртуальними транспортними засобами, що додає додаткового рівня занурення в ігровий процес.

17. VR Окуляри-шолом: VR окуляри-шолом надають користувачам можливість досліджувати віртуальні світи, відчувати присутність у них та отримувати унікальний досвід, який важко відтворити за допомогою звичайного монітора.

Таблиця 2.1 – Специфікація обладнення.

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітки
1	Головний сервер: Intel Xeon E-2236, 32GB RAM, 2TB HDD, 240GB SSD	Cisco UCS C220 M5 Server	од.	1	Центральний сервер

Продовження табліці 2.1

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітки
2	Сервер баз даних: Intel Xeon E-2276M, 64GB RAM, 4TB HDD, 500GB SSD	Cisco UCS C240 M5 Server	од.	1	Для зберігання і управління базами даних
3	Файловий сервер: Intel Xeon E-2224, 16GB RAM, 8TB HDD	Cisco UCS C240 M5 Server	од.	1	Для зберігання файлів та резервних копій
4	Сервер аутентифікації: Intel Xeon E-2226G, 16GB RAM, 500GB SSD	Cisco UCS C240 M5 Server	од.	1	Для управління доступом користувачів
5	Комутатор: 24 портів, 1GbE, управління L2/L3	Cisco Catalyst 2960-24TT	од.	8	Об'єднання робочих станцій в єдину мережу
6	Маршрутизатор: 2 порти WAN, 4 порти LAN, VPN підтримка	Cisco 2911 Integrated Services Router	од.	8	Забезпечення доступу до Інтернету
7	Бездротова точка доступу: Dual-Band, 802.11ac, MU-MIMO	Cisco Aironet 3700 Series	од.	3	Забезпечення бездротового підключення
8	Ігрова станція: Intel Core i7-10700K, 16GB RAM, 1TB SSD, NVIDIA GeForce RTX 3070	ASUS ROG Strix	од.	40	Для запуска ігор
9	Адміністративна станція: Intel Core i5-10400, 8GB RAM, 512GB SSD	Dell OptiPlex 7070	од.	2	Для адміністраторів клубу
10	Системна станція: Intel Core i3-10100, 8GB RAM, 256GB SSD	HP EliteDesk 800 G5	од.	2	Для технічного обслуговування
11	Мережевий файрвол: Stateful firewall, 1Gbps throughput	Cisco ASA 5506-X	од.	1	Захист від зовнішніх загроз

Продовження табліці 2.1

12	Система виявлення та запобігання вторгненням: IPS/IDS, 1Gbps throughput	Cisco Firepower 1010	од.	1	Моніторинг та захист мережі
14	LAN-кабель 60 метрів	OK-Net	од.	1	Підключення локальної мережі
15	IoT прилади: Світлодіоди (2 од.) DLC100 (Керування кібер фізичною системою 1 од.) Електро лампа (1 од.) Ветилятори (3 од.) LCD (1 од.) Температурний сенсор (1 од.) Датчик руху (2 од.)		Од.	1	Для впровадження робочої кібер фізичної
16	WAN-кабель 40 метрів	ОдесКабель	од.	1	Для підключення маршрутизаторів
17	RJ-45 з'єднувач	EServer	од.	32	Для підключення кабелів Ethernet
18	Провідний джойстик	Logitech X-56 Rhino Saitek Pro	од.	20	Для впровадження працездатної кіберфізичної системи
19	Проводной руль	Logitech G29 Driving Force PC	од.	20	Для впровадження працездатної кіберфізичної системи
20	VR Окуляри-шолом	SHINECON VR SC-G02ED	од.	20	Для впровадження працездатної кіберфізичної системи

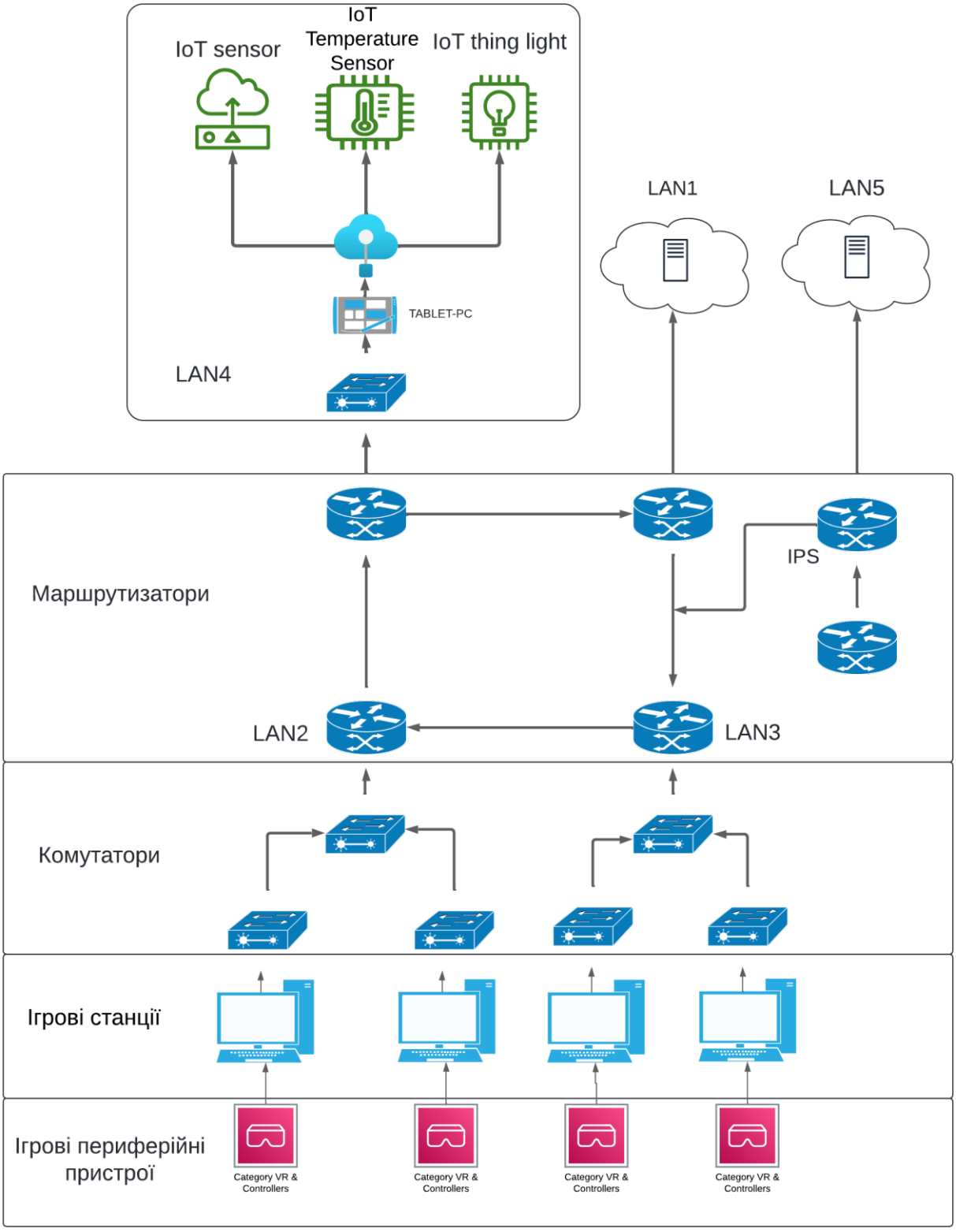

Рисунок 2.5 – Структурна схема технічних засобів кіберфізичної системи

2.7 Розрахунок вхідного трафику найбільшої локально мережі

Найбільшою мережею у комп'ютерному клубі є головний ігровий зал (LAN 4). Дані для розрахунку вхідного трафіку:

– кількість вузлів: N = 109;

– середня інтенсивність трафіку: I = 113 μ;

– затримка передачі пакету: D = ≤5;

– кількість портів комутатору: Ps = 48;

– середня довжина повідомлення: L = 600 байт;

Пропускна здатність P в бітах на секунду (біт/с) за формулою:

$$P=N\times I\times D\div Ps\times L\times 8$$

N - Кількість вузлів (109),

I - середня інтенсивність трафіку (113 μ),

D - Затримка передачі пакету (5),

Ps- кількість портів комутатора (48),

L - Середня довжина повідомлення у байтах (600).

$$P = 109\times 113\times 5\div 48\times 600\times 8$$

$$P = 620845\div 28800\times 8$$

$$P \approx 21,54\times 8$$

$$P \approx 172,32$$

Пропускна здатність P становить приблизно 172,32 біта на секунду.

Формула для визначення інтенсивності виходу. При розрахунку враховується, що навантаження на комутаторі рораховується через лінію 1000 мбіт/с.

$$\lambda_{out} = \lambda_{in}\times L/C$$

λ_{out} − інтенсивність виходу (пакетів/сек)

λ_{in} − інтенсивність входу (пакетів/сек)

L − середня довжина повідомлення (біти)

C − пропускна здатність каналу (біт/с)

З нашими даними:

$$\lambda_{in} = 113\mu \text{ (пакетів/сек)}$$

$$L = 600 \text{ байт} \times 8 = 4800 \text{ біт}$$

$$C = 1000 \text{ мбіт/с} = 1000000000 \text{ біт/с}$$

Формула для визначення максимальної кількості вузлів, яку можна підключити до комутатора рівня розподілу, на основі заданої середньої інтенсивності трафіку може бути наступною:

$$N = C \times l/\lambda$$

де:

N - Максимальна кількість вузлів,

C - Ємність лінії (у бітах на секунду),

I - середня інтенсивність трафіку (у бітах на секунду),

λ - Середня довжина повідомлення (у бітах).

Враховуючи, що дані середньої інтенсивності трафіку I і середньої довжини повідомлення λ вже мають одиниці бітів на секунду, формула спрощується до: $N = C/\lambda \times I$

В даному випадку $C = 1000 \times 10^6$

$$C = 1000 \times 10^6 \text{ біт на секунду (1 Гбіт/с), I=113×106}$$

$$I = 113 \times 10^6 \text{ біт на секунду, а } \lambda=600$$

$$\lambda = 600 \text{ байт або } 600 \times 8$$

Підставляючи ці значення в формулу, отримаємо:

$$N = 1000 \times 10^6/600 \times 8 \times 113 \times 10^6$$

$$N = 260416.6667 \times 113000000$$

$$N = 29416666666.7$$

$$N = 29.7$$

Формула для розрахунку середньої довжини черги виглядає наступним чином:

$$\rho = \lambda/c \times S$$

λ - Інтенсивність вхідного потоку (запити на одиницю часу)

c - Кількість обслуговуючих пристроїв (каналів)

S - Середній час обслуговування одного запиту

Пропускна здатність каналу визначається як обсяг даних, що можуть бути передані через канал зв'язку за одиницю часу. Формула для визначення пропускної здатності:

$$C= L\times N\times\lambda\times\tau/L$$

C − пропускна здатність каналу (біт/с)

N − кількість вузлів

λ − середня інтенсивність трафіку (пакетів/сек)

τ − середня затримка передачі пакету (сек)

L − середня довжина повідомлення (байт)

Підставляючи значення:

$$N = 109$$

$$\lambda = 113\mu \text{ (пакетів/сек)}$$

$$\tau \leq 5\text{мс} = 0.005\text{с}$$

$$L = 600 \text{ байт}$$

$$C = 109\times113\times0.005/600 = 615.45/600 \approx 1.02575 \text{ біт/с}$$

$$C = 1.025 \text{ біт/с}$$

Формула загальної інтенсивності трафіку визначається:

$$\mathbf{\Lambda=N\times\lambda\times L}$$

Λ − загальна інтенсивність трафіку (біт/с)

N − кількість вузлів

λ − середня інтенсивність трафіку на вузол (пакетів/сек)

L − середня довжина повідомлення (біти)

Підставимо дані у формули:

N = 109

λ = 113μ (пакетів/сек)

$$L = 600 \text{ байт} \times 8 = 4800\text{біт}$$

$$\Lambda = 109 \times 113 \times 4800 = 59342400 \text{ біт/сек}$$

Загальна інтенсивність трафіку становить 59,342,400 біт/с (або приблизно 59.34 Мбіт/с).

Формула коефіцієнта затримки на рівні розподілу може визначатися через коефіцієнт використання каналу та середній час обслуговування:

$$D = \lambda \times Ts / 1 - \lambda \times Ts$$

D − коефіцієнт затримки

λ − інтенсивність вхідного трафіку (пакетів/сек)

Ts − середній час обслуговування (секунд/пакет)

$$\lambda = 113\mu$$

$$Ts = 8 \times 10\text{^}-9 \text{ сек/пакет}$$

$$D = 113 \times 8 \times 10\text{^}-9 / 1 - 113 \times 8 \times 10\text{^}-9$$

$$D \approx 9.04 \times 10\text{^}-7$$

Коефіцієнт затримки D виявляється дуже малим, що свідчить про високу ефективність мережі при таких параметрах.

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Розрахунок адресації комп’ютерної мережі

Згідно з поставленною задачею ми маємо наступні вхідні значення блоку адрес та кількість вузлів. Ці значення ми будемо використовувати у написанні робочоі комп’ютерної моделі клубу. Всього в нас є 332 вузла.

Таблиця 3.1 – Блок адрес та кількість вузлів використовуемих комп’ютерним клубом «СКАЛА»

Блок адрес:	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
10.25.128.0/22	36	85	99	100	39

Посилаючісь до архіктури підприємства яку ми маємо (Рисунок 2.2), можно зрозуміти як треба розробляти нажу мережу. Розумною ідеєю буде використовувати программу Cisco packet tracer, у якому є всі необхідні нам пристро**їй,** а також можливість создати робочу модель.

Гарним рішенням за для розбиття нашоі мережі на декілька інших підмереж буде використання методу маски змінної мережі скорочено – VSLM, цей метод дозволяє розмір у двійкову ступінь. Тобтоб беремо саму велику мережу це LAN 4(100). За правилом, нам потрібно ігнорувати 8біт з правої сторони рядка. Таким чином ми получаємо підмережу 10.25.128.0/22. Діапозон IP-адрес хостів 10.25.128.1 – 10.25.131.254. Однак 10.25.131.255 широкомовна адреса, яку неможливо надати ніякому з вузлів бо вона розсилає пакети на всі підключені вузли своєї мережі.

Таблиця 3.2 – Схема адресації мережі

Назва підмережі	Кількість вузлів	Адреса	Префікс	Діапазон доступних адрес
LAN 1	36	10.25.129.19	26	10.25.129.193 – 10.25.129.254
LAN 2	85	10.25.129.0	25	10.25.129.193 – 10.25.129.254
LAN 3	99	10.25.128.128	25	10.25.129.1 – 10.25.129.126
LAN 4	100	10.25.128.0	25	10.25.128.1 – 10.25.128.126
LAN 5	39	10.25.129.128	26	10.25.129.129 – 10.25.129.190

Таблиця 3.3 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Інтерфейс підключеного пристрою
Sorocopud_Router1	g0/0	64.100.13.1	/30	fa0/0
	g0/1	10.25.80.193	/28	eth6
Sorocopud_Router2	fa0/0	10.25.80.129	/25	fa0/2
	fa0/1/0	10.1.12.1	/30	fa0/0
	se0/3/0	10.25.80.65	/25	eth6
	fa0/1	10.1.12.2	/30	fa0/1
Sorocopud_Router3	fa0/0	10.25.80.1	/26	fa0/5
	se0/2/0	10.1.12.5	/30	se0/2/0
Sorocopud_Router4	se0/3/0	10.1.12.9	/30	se0/2/0
	se0/1/1	209.165.202.0	/30	se0/2/1
	fa0/0	10.25.80.209	/28	eth6
Sorocopud_RouterIPS	Gig0/0		/28	fa0
	Gig0/1	64.100.13.0	/30	g0/0
	se0/0/1	209.165.202.0	/30	se0/2/1

В таблиці 3.4 ми записали IP-адреси, які ми получили за формулою виданою замовником (перша адреса підмережі + 9 + № варіанта),

10.25.128.0 + 9 + 10 = 10.25.128.19

Таблиця 3.4 – IP-адреси комутаторів

Підмережа	Пристрій	IP-адреса	Маска	Шлюз	VLAN
LAN1	Sorocopud_Switch0			10.25.129.124/26	
	Sorocopud_Switch1				
	Sorocopud_Switch2				
LAN2	Sorocopud_Switch3			10.25.129.2/26	
	Sorocopud_Switch4				
LAN3	Sorocopud_Switch5			10.25.128.227/26	
	Sorocopud_Switch6				
LAN4	Sorocopud_Switch7			10.25.128.2/25	
LAN5	Sorocopud_Switch8			10.25.129.124/26	

Таблиця 3.5 – Адресація інтерфейсів серверів

Назва серверу	Назва інтерфейсу	IP-адреса	Маска	Шлюз
Sorocopud_ServerDNS	Fa0	10.25.128.218	255.255.255.224	10.25.128.193
Sorocopud_ServerTFTP	Fa0	10.25.128.26	255.255.255.128	10.25.128.1
Sorocopud_ServerHTTP	Fa0	10.25.129.218	255.255.255.192	10.25.129.193

3.2 Модель корпоротивної мережі комп’ютерного клубу «СКАЛА»

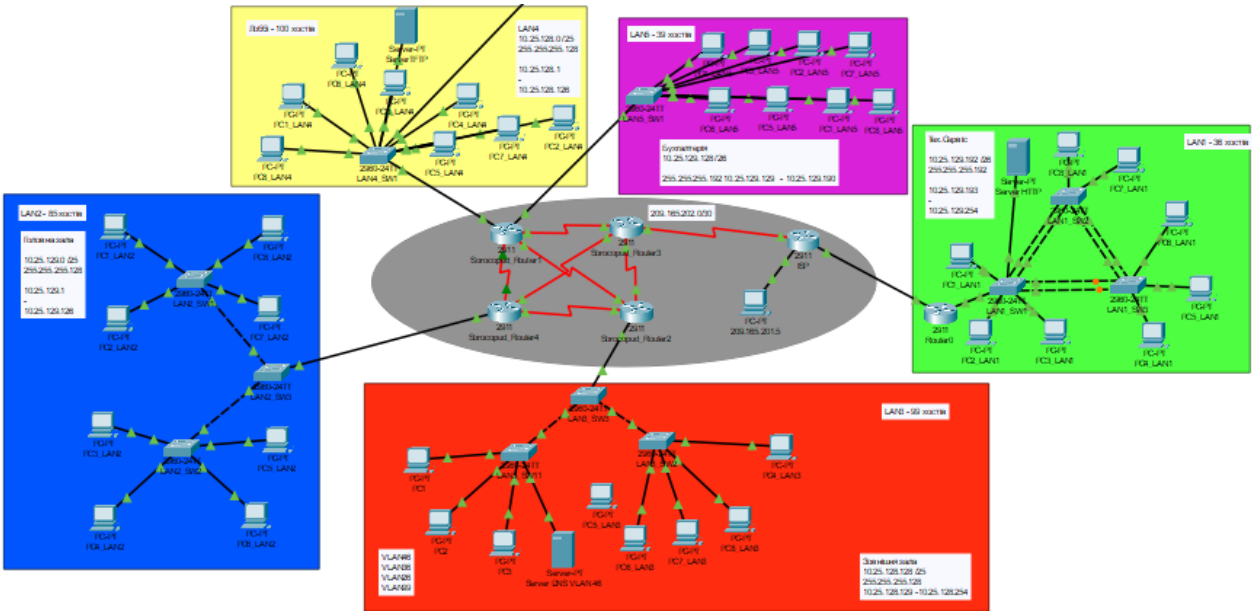

Рисунок 3.1 – Модель корпоротивної мережі комп’ютерного клубу

Підготувавши всі теоритичні та вводні данні (Таблиця 3.1 – 3.5) можно починати портувати все що ми получили до програми Cisco packet tracer, за для формування кібер физичної системи у межах цієї програми. Завдяки їй ми побачимо помилки(якщо вони є) у нашій мережі. Портована модель виглядає таким чином:

3.3 Налаштування пристроїв конфігуряції

Виконуємо налаштування конфігурації пристроїв мережі для захисту. Проведемо ці налаштування на прикладі маршрутизатора підмережі LAN1.

Router>en

```
Router#conf t
Router(config)#hostname Sorocopud_Router_1
```

```
LAN1 Sorocopud_Router_1(config)#line console 0
Sorocopud_Router_1(config-line)#password cisco
Sorocopud_Router_1(config-line)#login
Sorocopud_Router_1(config-line)#line vty 0 8
Sorocopud_Router_1(config-line)#password cisco
Sorocopud_Router_1(config-line)#login
Sorocopud_Router_1(config-line)#enable secret class
Sorocopud_Router_1(config)#service password-encryption
Sorocopud_Router_1(config)#banner   motd   "Hi!   I'mSorocopud_Router_1.
Let'sdo it!"
Sorocopud_Router_1(config)#ip domain-name Sorocopud_Router_1
Sorocopud_Router_1(config)#crypto key generate rsa
52How many bits in the modulus [512]: 1024
Sorocopud_Router_1(config)#username 123201_Sorocopudpasswordadmincisco
Увімкнено використання протоколу ssh на всіх vty лініях:
Sorocopud_Router_1(config)#line vty 0 8
Sorocopud_Router_1(config-line)#transport input ssh
Sorocopud_Router_1(config-line)#login local
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Sorocopud_Router_1
Sorocopud_Router_1(config)#line console 0
Sorocopud_Router_1(config-line)#password cisco
Sorocopud_Router_1(config-line)#login
Sorocopud_Router_1(config-line)#line vty 0 8
Sorocopud_Router_1(config-line)#password cisco
Sorocopud_Router_1(config-line)#login
Sorocopud_Router_1(config-line)#enable secret class
Sorocopud_Router_1(config)#service password-eneryption
                                                  ^
% Invalid input detected at '^' marker.

Sorocopud_Router_1(config)#service password-encryption
Sorocopud_Router_1(config)#banner motd "Hi! I'mSorocopud_Router_1.Let'sdo it!"
Sorocopud_Router_1(config)#ip domain-name Sorocopud_Router_1
Sorocopud_Router_1(config)#crypto key generate rsa
The name for the keys will be: Sorocopud_Router_1.Sorocopud_Router_1
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Sorocopud_Router_1(config)#username 123201_Soropudpasswordadmincisco
*Mar 1 0:24:7.576: %SSH-5-ENABLED: SSH 1.99 has been enabled
Sorocopud_Router_1(config)#line vty 0 8
Sorocopud_Router_1(config-line)#transport input ssh
Sorocopud_Router_1(config-line)#login local
Sorocopud_Router_1(config-line)#
```

Рисунок 3.2 – Налаштування конфігурації пристроїв мережі

3.4 Налаштування маршрутизаторів корпоративної мережі

Для забезпечення взаємодії між клієнтами та пристроями у мережі, на маршрутизаторах були налаштовані відповідні IP-адреси на інтерфейсах. Після цього була конфігуровано таблиця маршрутизації на кожному з них таким чином, щоб кожен пристрій з однієї підмережі міг встановлювати зв'язок з будь-яким іншим у своїй або чужій підмережі.

Для створення таблиці маршрутизації ми використали протокол RIP. Це універсальний протокол, який підтримується практично на всіх моделях маршрутизаторів. Щодо його особливостей, протокол RIP розсилає повну таблицю маршрутизації через всі активні інтерфейси кожні 30 секунд, що зменшує його ефективність у порівнянні з більш сучасними аналогами. Також важливо враховувати обмеження на кількість переходів між маршрутизаторами. Проте його простота в налаштуванні у мережі і універсальність порівняно з протоколами, роблять RIP зручним і оптимальним вибором для нашої невеликої мережі. Під час створення таблиць маршрутизації, ми використали статичну маршрутизацію на наших граничних маршрутизаторах для забезпечення доступу до основної мережі та внутрішньої комунікації, а також налаштували вихід пристроїв мережі підприємства в Інтернет. Налаштування протоколу RIP (LAN2) протоколу:

```
Sorocopud_Router_1(config)#router rip
Sorocopud_Router_1(config-router)#version 2
Sorocopud_Router_1(config-router)#network 10.24.80.0
Sorocopud_Router_1(config-router)#network 10.24.80.128
Sorocopud_Router_1(config-router)#exit
```

Передача оновленої інформації протоколом RIP на інші маршрутизатори мережі виглядає наступним чином:

```
Sorocopud_Router_1(config)#router rip
Sorocopud_Router_1(config-router)#version 2
Sorocopud_Router_1(config-router)#network 10.24.80.0
Sorocopud_Router_1(config-router)#network 10.24.80.128
Sorocopud_Router_1(config-router)#exit
Sorocopud_Router_1(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.2
Sorocopud_Router_1(config)#router rip
Sorocopud_Router_1(config-router)#redistribute static
```

Додаємо статичний маршрут для забезпечення доступу з локальної мережі підприємства до мережі провайдера ISP.

```
Sorocopud_Router_1 (config)#ip route 209.165.201.0 255.255.255.240
209.165.202.2
```

Згідно з вимогами, задаємо пропускну спроможність та тактову частоту на маршрутизаторах:

```
Sorocopud_Router_1(config-if)#clock rate 128000
Sorocopud_Router_1 (config-if)#bandwidth 128
```

Налаштування служби AAA виглядає таким чином:

```
Sorocopud_Router_1(config)#aaa new-model
Sorocopud_Router_1(config)#radius-server host 10.24.80.128 auth-port 1645key radius123
```

Створюємо локальну базу даних згідно з вимогами:

```
Sorocopud_Router_1(config)# aaa authentication login CONSOLE group radius local
Sorocopud_Router_1(config)# line console 0
Sorocopud_Router_1(config-line)# login authentication CONSOLE
Sorocopud_Router_1(config-line)# exit
Sorocopud_Router_1(config)# aaa authentication login default local
Sorocopud_Router_1(config)# username Sorocopud_Router_1 password admin123
Sorocopud_Router_1(config)# line vty 0 8
Sorocopud_Router_1(config-line)# login authentication default
Sorocopud_Router_1(config-line)# exit
Sorocopud_Router_1(config)# do write
```

Виконуємо останні налаштування на AAA-сервісі, розміщеному на DNS-сервері. Як показано на рисунку 3.8, до серверу RADIUS було додано всі маршрутизатори, а також створено єдиного користувача, який був зареєстрований на кожному з них.

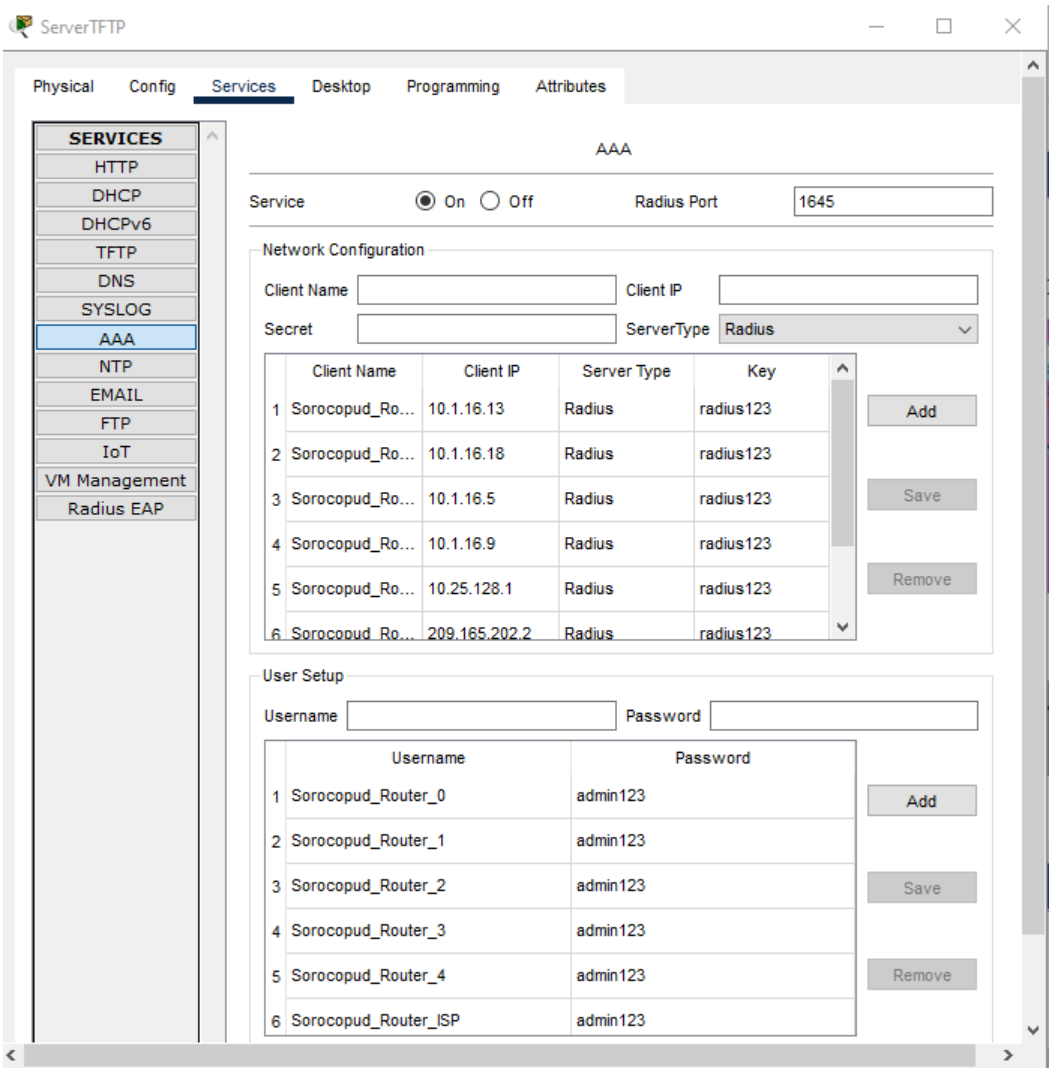

Рисунок 3.3 – Налаштування AAA на сервері

Кожен з маршрутизаторів був налаштований на динамічне розподілення адрес вузлам своєї підмережі. Для цього були створені DHCP пули адрес на кожному маршрутизаторі. Окремо були виключені адреси серверів підприємства, якщо вони входять до підмережі, для якої створюється пул адрес.

Налаштування такого пулу приведемо на прикладу LAN1:

```
Sorocopud_Router_1(config)#ip dhcp pool LAN1
Sorocopud_Router_1(dhcp-config)#network 10.24.80.0 255.255.248.128
Sorocopud_Router_1(dhcp-config)#default-router 10.24.80.1
Sorocopud_Router_1(dhcp-config)#dns-server 10.24.80.143
Sorocopud_Router_1(dhcp-config)#exit
Sorocopud_Router_1(config)#ip dhcp excluded-address 10.24.80.1
10.24.80.10
Sorocopud_Router_1(config)#ip dhcp excluded-address 10.24.80.15
```

3.5 Налаштування роботи Інтернет

Для забезпечення виходу пристроїв наших підмереж в Інтернет, ми налаштували динамічний NAT на граничному маршрутизаторі, використовуючи діапазон адрес від 209.165.200.5 до 209.165.200.30. Для цього було створено розширений список доступу NAT5, який блокує трафік з нашої основної мережі до віддалених мереж, але дозволяє весь інший трафік.

```
Sorocopud_Router_2(config)#ip access-list extended NAT5
Sorocopud_Router_2(config-ext-nacl)#deny    ip    10.24.80.0    0.0.0.255
10.24.80.128 0.0.0.127
Sorocopud_Router_2(config-ext-nacl)#deny    ip    10.24.80.128    0.0.0.127
10.23.34.128 0.0.0.127
Sorocopud_Router_2(config-ext-nacl)#deny    ip    10.24.84.0    0.0.0.255
10.23.34.128 0.0.0.127
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.80.0 0.0.0.255 any
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.81.0 0.0.0.127 any
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.82.0 0.0.0.127 any
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.83.0 0.0.0.127 any
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.84.0 0.0.0.255 any
```

Наступним кроком, користуючись цим списком, намибулоналаштовано інтерфейси на взаємодію з NAT:

```
Sorocopud_Router_2 (config)#int s0/0/1
Sorocopud_Router_2 (config-if)#ip nat inside
Sorocopud_Router_2 (config-if)#int s0/1/1
Sorocopud_Router_2 (config-if)#ip nat inside
Sorocopud_Router_2 (config-if)#int s0/1/0
Sorocopud_Router_2 (config-if)#ip nat inside
Sorocopud_Router_2 (config-if)#int g0/0
Sorocopud_Router_2 (config-if)#ip nat inside
Sorocopud_Router_2 (config-if)#int s0/0/0
Sorocopud_Router_2 (config-if)#ip nat outside
```

Створюм пулу Internet з адресами, вказаними у тех. вимогах, і призначення його для маскування IP-адрес пристроїв локальної мережі при їх виході у зовнішню мережу.

```
Sorocopud_Router_2(config)#ip nat pool Internet 209.165.200.5
209.165.200.30 netmask 255.255.255.224
Sorocopud_Router_2(config)#ip nat inside source list NAT5 pool Internet
```

Також нами булу створено два статичні NAT для DNS та HTTP серверів відповідно. Це потрібно для того, щоб користувачі могли за адресою http://123.dnipro. переглядати веб-сторінку нашого клубу.

```
Sorocopud_Router_2(config)#ip nat inside source static 10.24.80.143
209.165.200.4
Sorocopud_Router_2(config)#ip nat inside source static 10.24.80.15
209.165.200.3
```

Аналогічно, ми налаштували NAT на маршрутизаторі віддаленої мережі, використовуючи діапазон зовнішніх адрес 209.165.200.37 - 209.165.200.62 з маскою 255.255.255.224

Для налаштування безпечного, зв'язку між ними, буде використано VPN з використанням IPsec для трафіку. На граничному маршрутизаторі та віддаленої мережі нами було активовано модуль securityk9:

```
Sorocopud_Router_2(config)#license boot module c2900 technology-package
securityk9
```

Далі нами було створено нові списки доступу – VPN8, що на відміну від списків NAT8, дозволятимуть проходження трафіку між основною мережею та віддаленою:

```
Sorocopud_Router_2(config)#ip access-list extended VPN5
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.80.0    0.0.0.255
10.24.80.128 0.0.0.127
SorocopudSorocopud_Router_2(config-ext-nacl)#permit     ip     10.24.81.0
0.0.0.127
10.24.81.128 0.0.0.127
SorocopudSorocopud_Router_2(config-ext-nacl)#permit    ip    10.24.82.128
0.0.0.127
10.23.34.128 0.0.0.127
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.24.83.   0 0.0.0.127
10.24.34.128 0.0.0.127
Sorocopud_Router_2(config-ext-nacl)#permit ip 10.0.5.0    0.0.0.255
10.24.81.128 0.0.0.127
```

створено загальний ключ шифрування soroc:

```
Sorocopud_Router_2(config)#crypto isakmp policy 10
Sorocopud_Router_2(config-isakmp)#encryption 3des
Sorocopud_Router_2(config-isakmp)#hash md5
Sorocopud_Router_2(config-isakmp)#authentication pre-share
Sorocopud_Router_2(config-isakmp)#group 2
Sorocopud_Router_2(config-isakmp)#crypto isakmp key soroc address
```

```
64.100.13.1
Sorocopud_Router_2(config)#crypto ipsec transform-set dokol esp-3des esp-
md5-hmac
Sorocopud_Router_2(config)#crypto map DMAP 10 ipsec-isakmp
Sorocopud_Router_2(config-crypto-map)#
Sorocopud_Router_2(config-crypto-map)#set peer 64.100.13.1
Sorocopud_Router_2(config-crypto-map)#set transform-set dokol
Sorocopud_Router_2(config-crypto-map)#match address VPN5
Sorocopud_Router_2(config-crypto-map)#exit
```

Прив'язавши створене криптографічне зіставлення DMAP до вихідного інтерфейсу граничного маршрутизатора. В результаті цього дії VPN-зв'язок було успішно активовано

3.6 Налаштування VLAN для захисту інформації в комп’ютерній

Для захисту інформації в системі від несанкціонованого доступу та розділення користувачів мережі на декілька підрозділів за виконуваними функціями, кожну мережу було розділено на чотири віртуальнілокальні мережі, три з яких, в свою чергу, належатимуть окремим відділам підприємства, а четверта – відповідати за управління пристроями мережі(Табл.3.9). Створення VLAN та призначення їм імен на прикладі центральногокомутатору мережі LAN3:

```
Sorocopud_Switch(config)#vlan 26
Sorocopud_Switch(config-vlan)#name VLAN26
Sorocopud_Switch(config-vlan)#vlan 36
Sorocopud_Switch(config-vlan)#name VLAN 36
Sorocopud_Switch(config-vlan)#name VLAN36
Sorocopud_Switch(config-vlan)#vlan 46
Sorocopud_Switch(config-vlan)#name VLAN46
Sorocopud_Switch(config-vlan)#vlan 99
Sorocopud_Switch(config-vlan)#name VLAN99
Sorocopud_Switch(config-vlan)#vlan 100
Sorocopud_Switch(config-vlan)#name VLAN100
Sorocopud_Switch(config-vlan)#
```

Таблиця 3.6 – Відомості про VLAN

Номер VLAN	Ім’я VLAN	Примітка	Розподілення портів
1	default	Не використовується	-
26	Accounting	Для бухгалтерії	f0/5 –f0/10
36	Tech Department	Для тех. підтримки	f0/10 –f0/15
46	Guest	Для гостей	f0/15 –f0/20
99	Management	Для управління пристроями	-
100	Native	Для управління пристроями	Switch: f0/1-3 та g0/1 Інші:f0/1

Окремо налаштовуємо як транковий порт, що відповідає за зв’язок з маршрутизатором:

```
Sorocopud_Switch(config)#int g0/1
Sorocopud _Switch(config-if)#switchport mode trunk
Sorocopud _Switch(config-if)#switchport trunk native vlan 100
```

Далі нами було VLAN налаштовано порти доступу (рис. 3.10) для кожної з користувацьких віртуальних мереж та транкові для мережі NATIVE:

```
% Invalid input detected at '^' marker.

Sorocopud_Switch(config-if-range)#int r f0/5-10
Sorocopud_Switch(config-if-range)#switchport mode access
Sorocopud_Switch(config-if-range)#int r f0/5-24
Sorocopud_Switch(config-if-range)#switchport mode access
Sorocopud_Switch(config-if-range)#switchport access vlan 46
Sorocopud_Switch(config-if-range)#int r f0/1-3
Sorocopud_Switch(config-if-range)#switchport mode trunk
```

Рисунок 3.4 – Налаштовано порти доступу

3.7 Перевірка роботи моделі комп’ютерної системи

Для перевірки базових налаштувань пристроїв та працездатності AAA сервісу, спробуємо зробити вхід до якогось з маршрутизаторів (Рис. 3.11):

```
Hi! I`m Sorocopud_Router3! Let`s do it!

User Access Verification

Username: 123201_Sorocopud
Password:
Sorocopud_Router_3>
```

Рисунок 3.5 – Вхід до Router3

Наступним кроком перевіримо можливість пристроїв мережі виходитиу інтернет. (рис. 3.12) Для цього на PC1 відправимо ехо-запит.

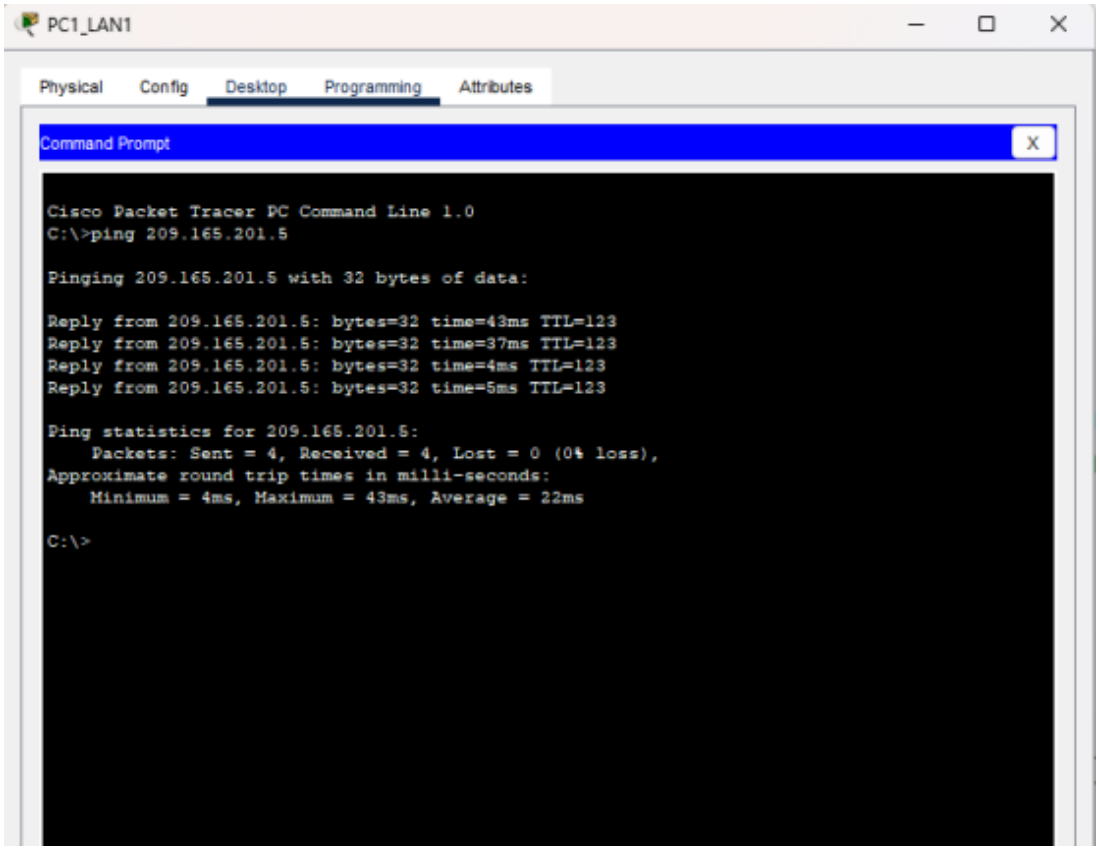

Рисунок 3.6 – Перевірка можливості пристроїв мережі виходити у інтернет

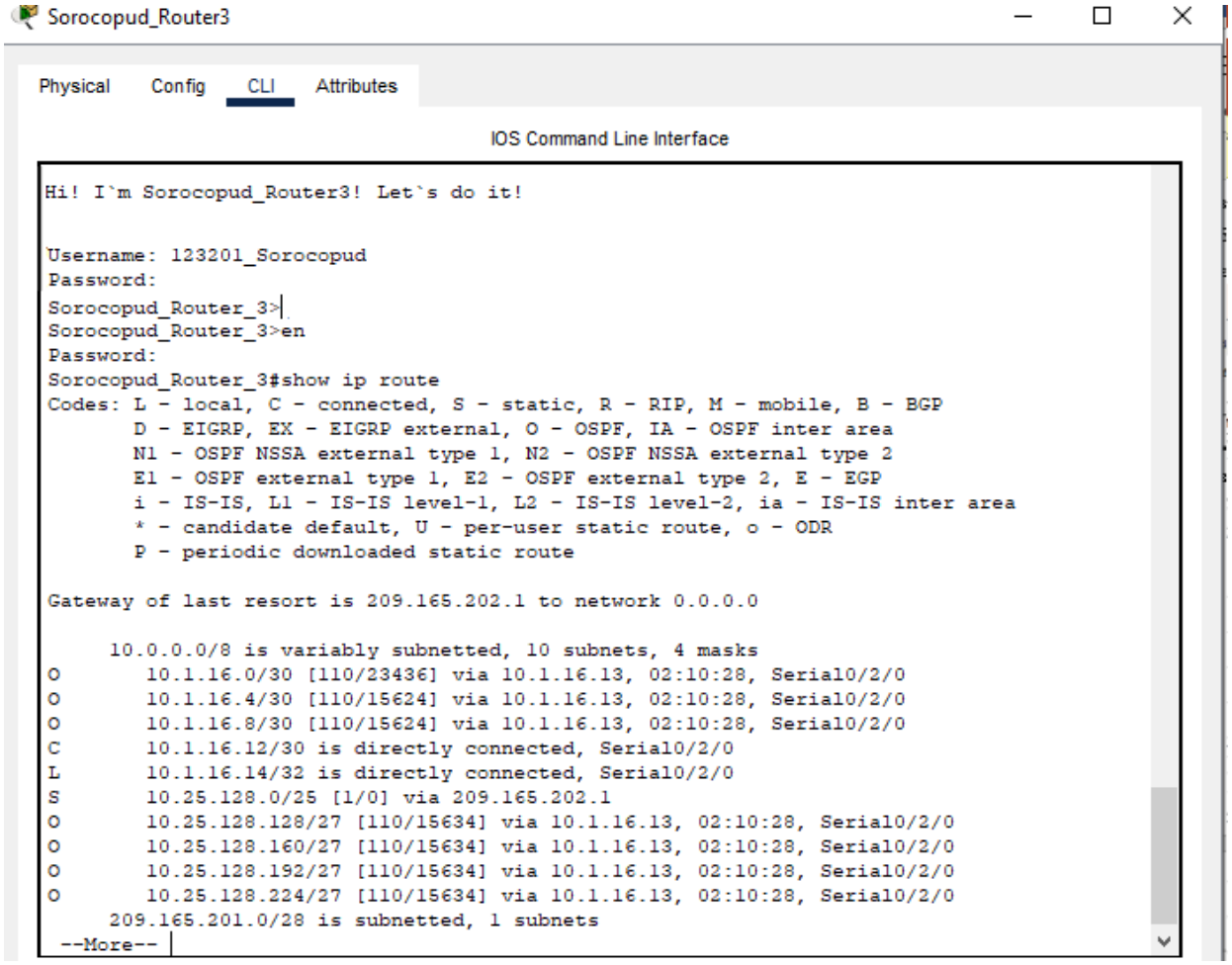

Рисунок 3.7 – Таблиця маршрутизації

Перевіримо доступність сайту комп.клубу «СКАЛА» з пристрою провайдера та йогонаповнення,що має включати тему, мету та завдання дипломного (Рис. 3.14).

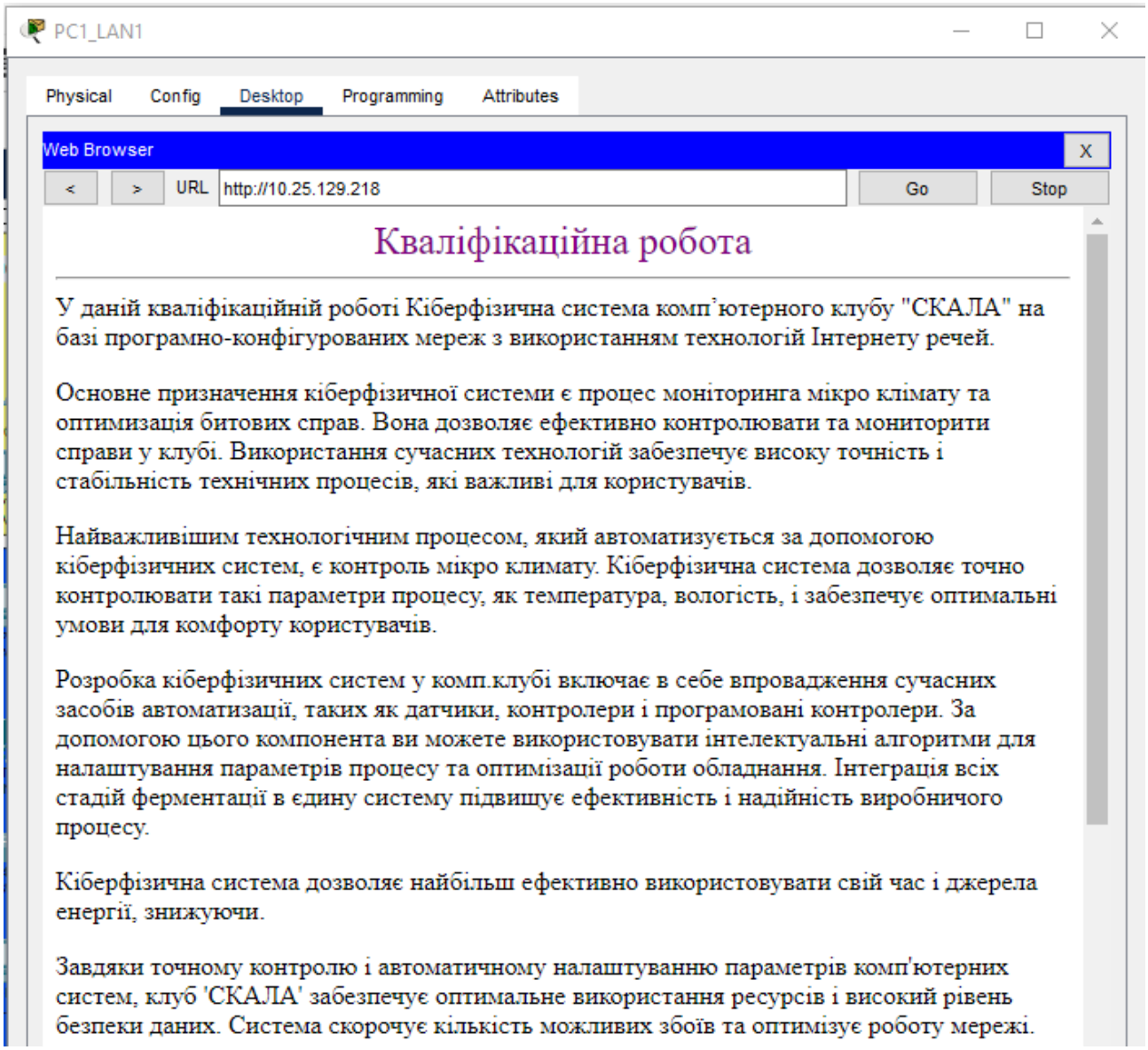

Рисунок 3.8 – Сайт комп`ютерного клубу «СКАЛА»

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Об'єкт та тип впроваджувального компоненту системи.

Для комп'ютерного клубу «СКАЛА» було розроблено кіберфізичну систему управління та моніторингу для забезпечення високого рівня комфорту та ефективності обслуговування клієнтів. Згідно з вимогами, система включає в себе контролер, автоматизоване управління обладнанням та контроль доступу до різних зон клубу.Нижче буде наведена топологія.

4.2 Застосовані технології IoT

В рамках проекту комп'ютерного клубу «СКАЛА» ми застосували технологію хмарних обчислень для забезпечення ефективного управління та моніторингу. За цією технологією обчислювальні ресурси надаються за запитом через мережу інтернет.

У нашому випадку обчислення здійснюватимуться на спеціально виділеному сервері IoT в мережі клубу, який фізично розташований поруч із сервером DNS та входить до тієї ж віртуальної локальної мережі VLAN36 для зручності доступу системного адміністратора. Цей сервер буде використовуватися для керування мікроклиматом в приміщеннях клубу та системою попередження про нявність кліенту.

Завдяки впровадженню хмарних обчислень та IoT технологій, комп'ютерний клуб «СКАЛА» забезпечує високий рівень ефективності та зручності, що сприяє створенню комфортного та сучасного ігрового середовища для клієнтів.

4.3 Розробка адресації та топології компоненту системи

Для забезпечення функціонування описаних компонентів ми додатково налаштували топологію мережі, пристрої, що виконуватимуть функції термометра, пристрої, необхідні для функціонування системи оповіщення про

наявність клієнтів у кімнаті, а також пристрій типу Home Gateway. Цей пристрій забезпечує бездротове підключення до IoT-пристроїв з одного боку, а з іншого. Логічну топологію отриманої мережі з розподілом пристроїв за поверхами розташування можна побачити на рисунку 4.1

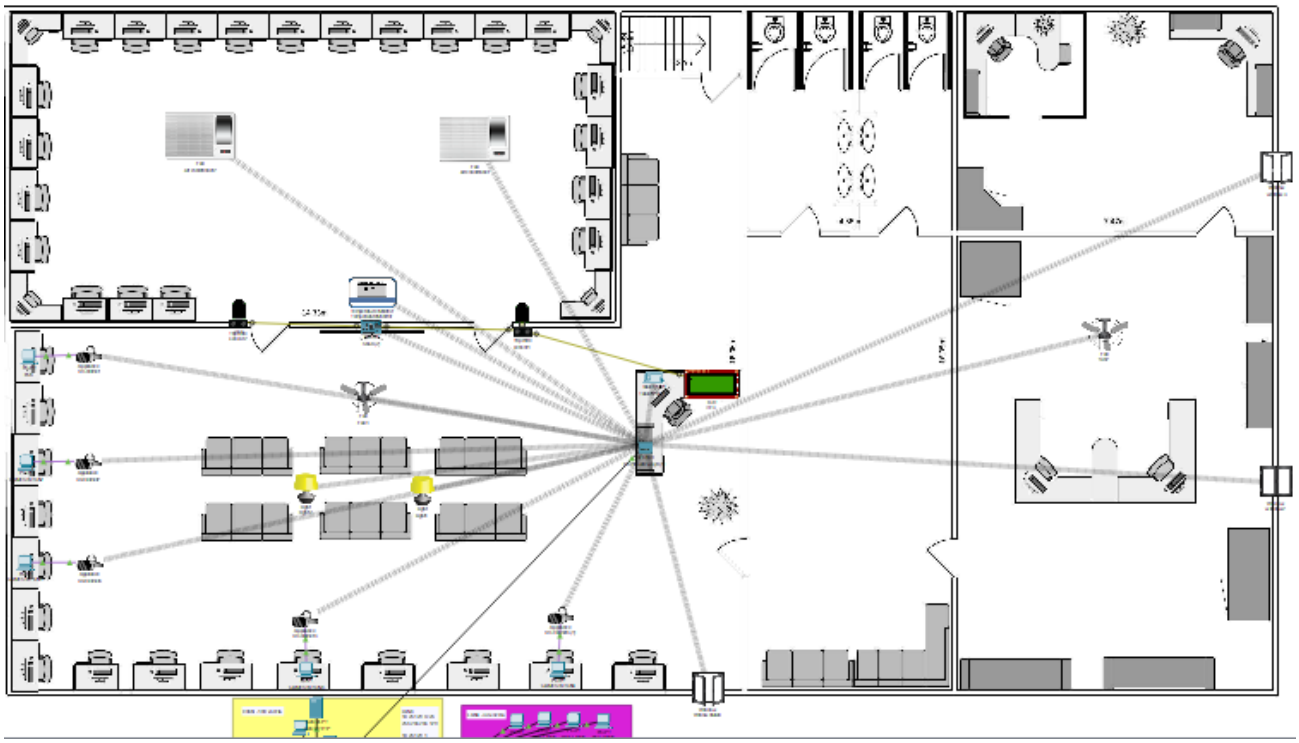

Рисунок 4.1 – Топологія компоненту системи

На рисунку 4.2 показано внутрішній шлюз для пристроїв, які підключаються зсередини, а також налаштування для можливої динамічної адресації внутрішніх пристроїв при увімкненні цієї опції. На рисунку 4.3 відображено мережеві налаштування, зокрема введено власний SSID мережі – HOME, а також встановлено протокол аутентифікації WPA2-PSK з паролем 123201SY. Це забезпечує певний захист від небажаних підключень до мережі та робить її приватною.

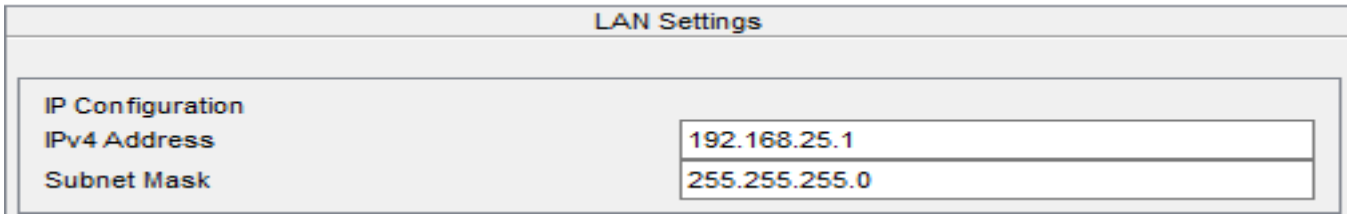

Рисунок 4.2 – Налаштування для можливої динамічної адресації

Принцип налаштування зв’язку з сервером у нашому випадку є однаковим для всіх пристроїв, оскільки ми використовуємо хмарні обчислення, і всі пристрої підключаються бездротово через спільний шлюз. У налаштуваннях бездротового зв’язку (Рис. 4.3) було зазначено SSID та пароль протоколу WPA2-PSK, які ми встановили на IoT шлюзі, а також обрано DHCP адресацію, щоб шлюз автоматично надав пристрою IP-адресу.

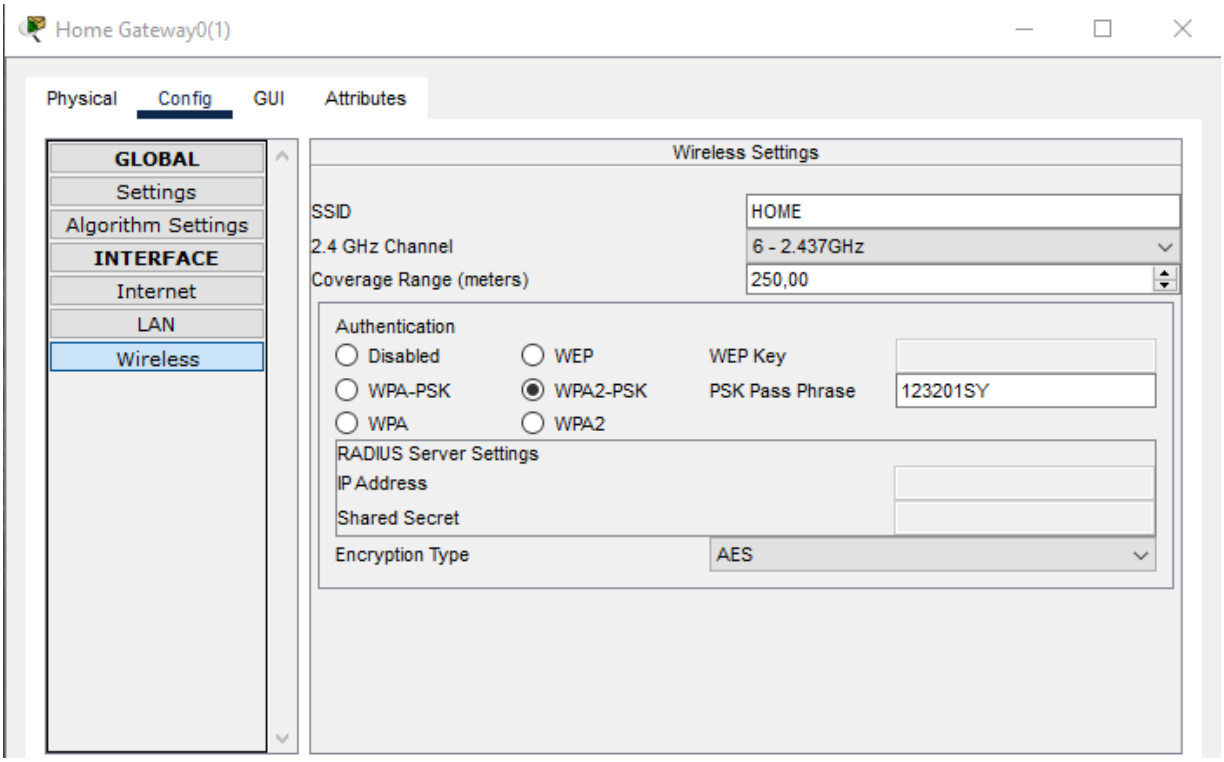

Рисунок 4.3 – Налаштування бездротового зв’язку

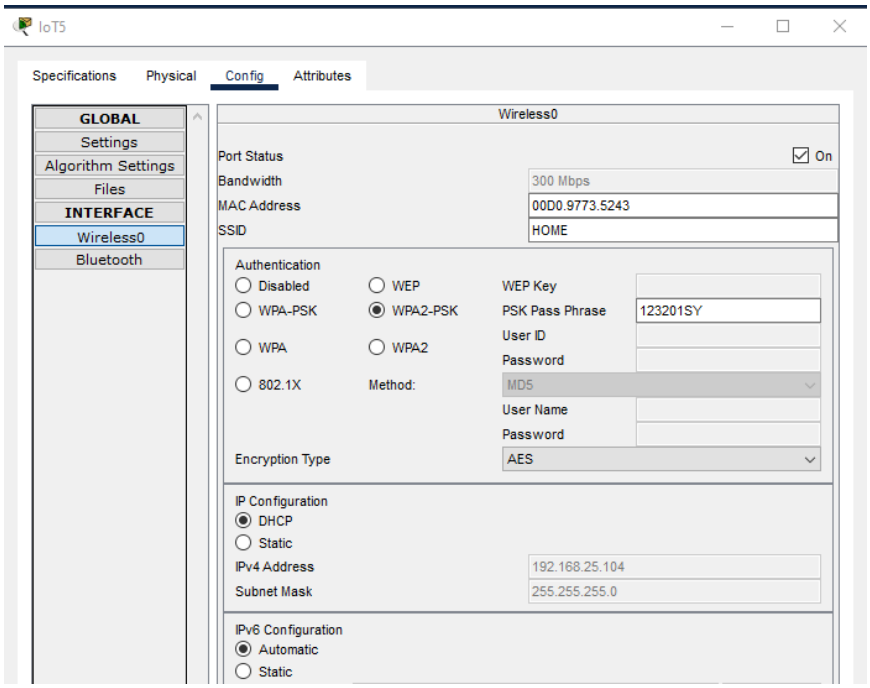

Рисунок 4.4 – Бездротові налаштування пристроїв IoT

Для налаштування та управління пристроями IoT, ми зможемо зайти з будь-якого ПК, підключеного до мережі підприємства, до нашого облікового запису на IoT сервері (Рис. 4.6). Там ми будемо мати доступ до списку всіх підключених пристроїв, їх поточний статус і зможемо вручну керувати їх функціями, особливо якщо це активні пристрої, такі як камери відеоспостереження та сирени. Таким чином ми закінчили налаштування кіберфізичної системи IoT.

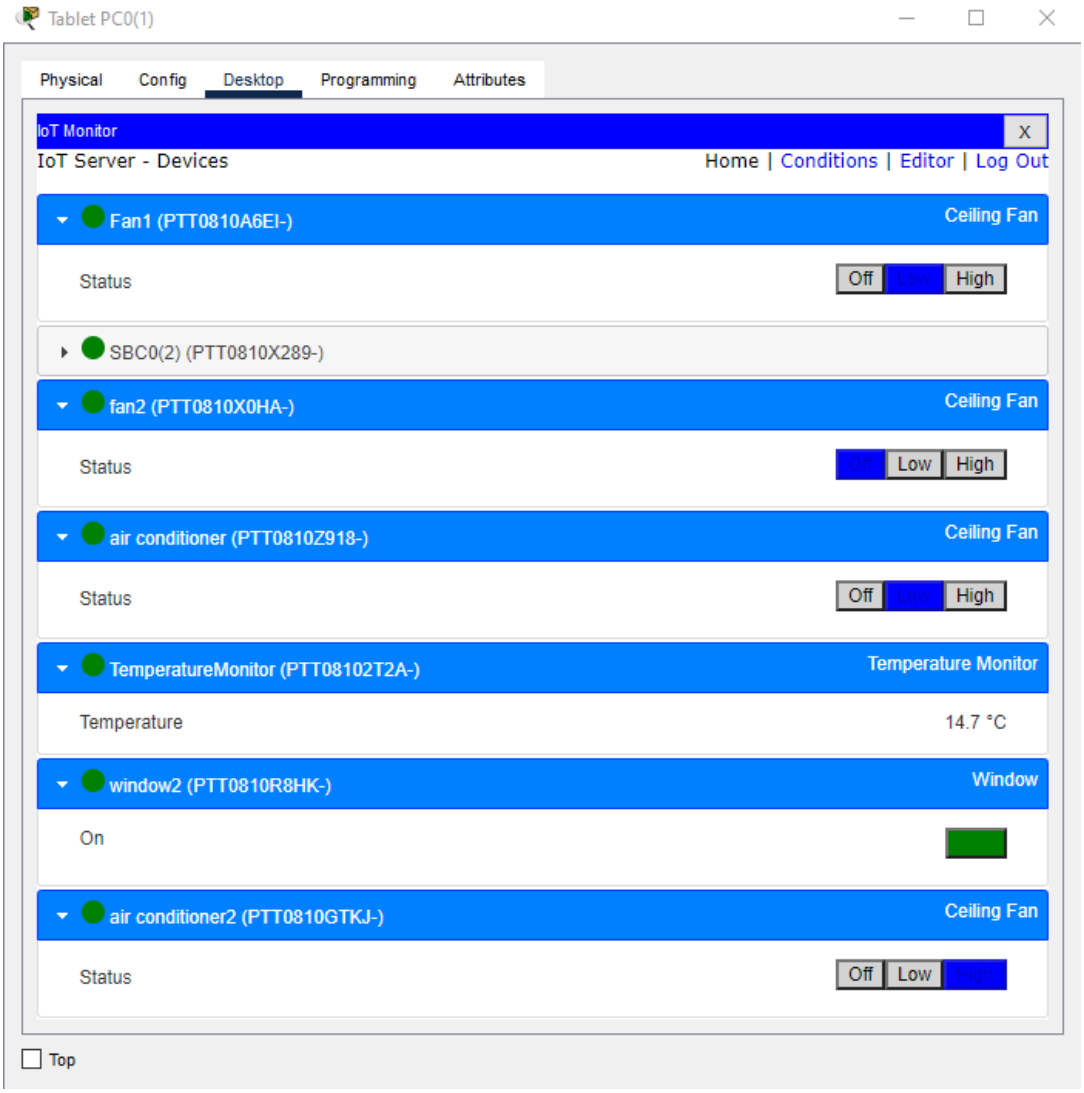

Рисунок 4.5 – Підключені та функціонуючі до IoT серверупристроїв

4.4 Налаштування ігрових периферійних пристроїв

Для налаштування спецільних контролерів та шолому віртуальної реальності нам потрібно зробити наступне:

1. Приєднати пристрій до ігрової станції (рис. 4.7)

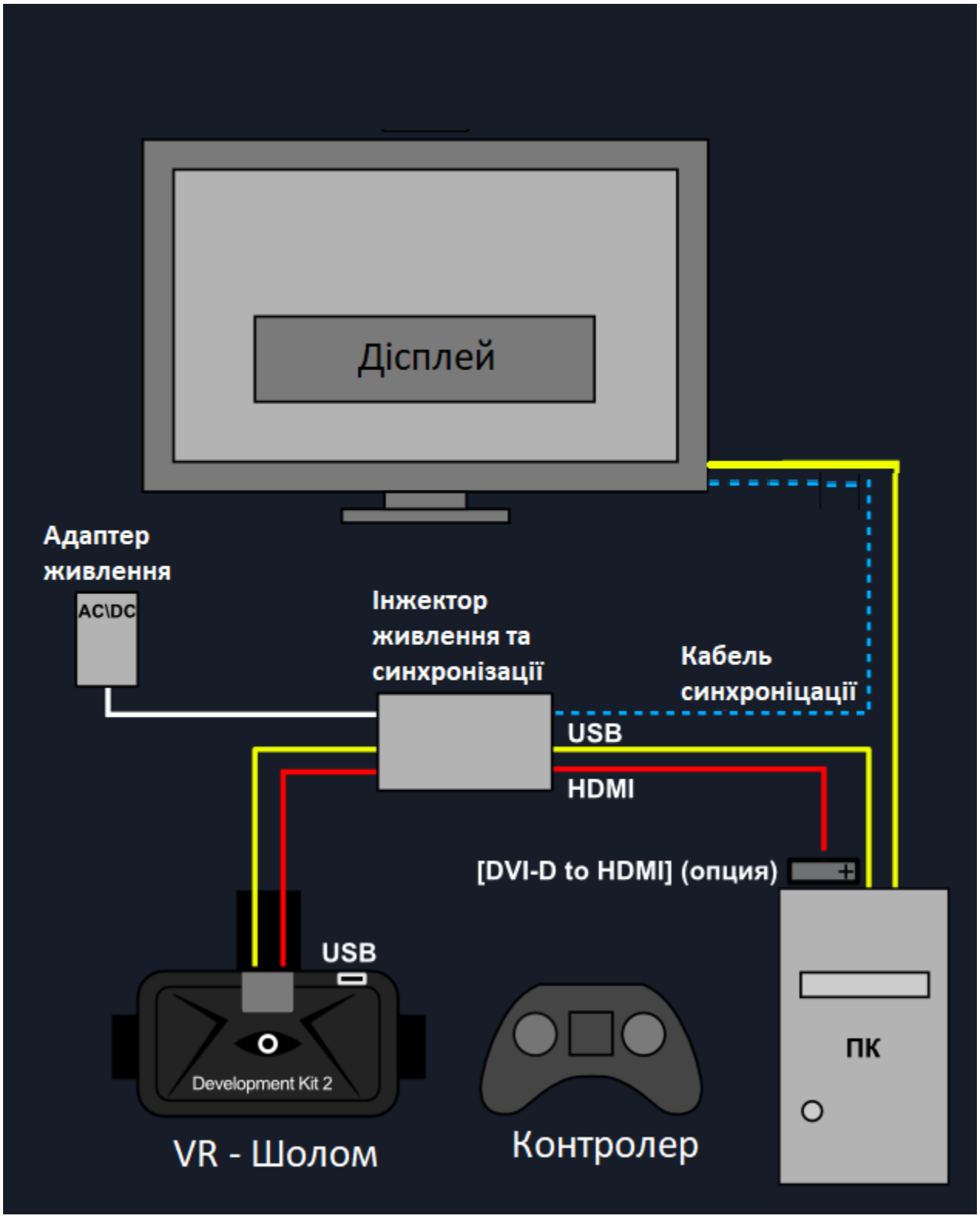

Рисунок 4.6 – Схема підключення

2. Включити його

3. Завантажити ПЗ для спеціального пристрою (рис. 4.7 підключення VR-шолому) Програмне забезпечення Oculus, також відоме як Oculus Home або

Oculus App, необхідне для керування гарнітурою віртуальної реальності Oculus і доступу до контенту VR.

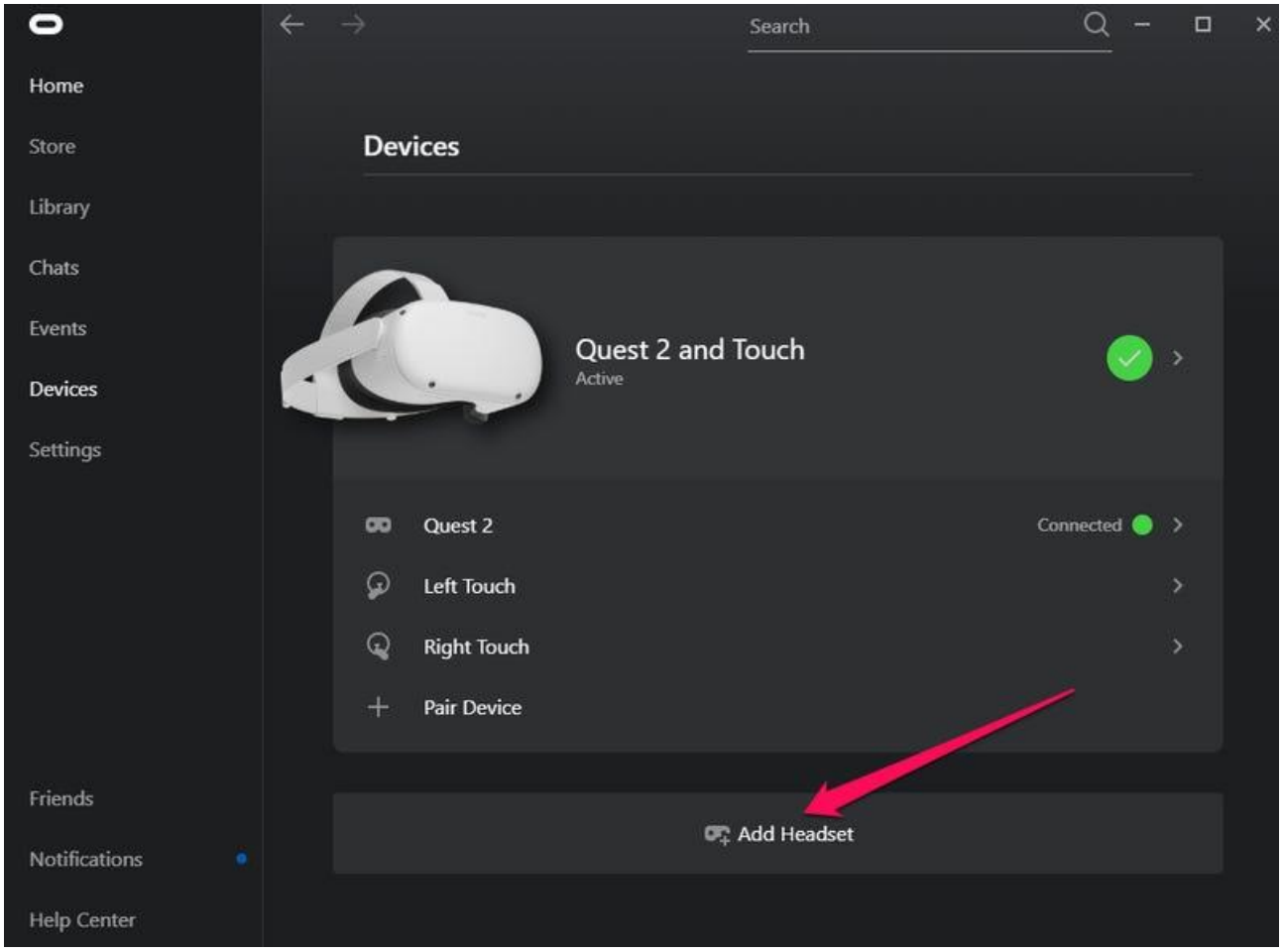

Рисунок 4.7 – Підключення VR-шолому до ПЗ Oculus

4. Виконати налаштування під конкретного користувача (рис. 4.7)

Додаток повинен автоматично знайти контролери та синхронізувати їх з гарнітурою, коли синхронізація успішна, можно буде побачити підтвердження на екрані додатку.

Повторять процес для кожного контролера, якщо використовується більше одного.

Рисунок 4.8 – Налаштування гарнітури у додатку

5. Запустити обраний симулятор або гру та почати занурення у дивний світ віртуальної реальності.

Завдяки такому налаштуванню, ми предоставимо користувачам найліпшого персонального досвіту з використування ношої мережі з можливих. Треба зазначити що такі кіберфізичні вироби які ми обрали у технічних вимогах будуть як найкраще доповнювати один-одного та будуть витримивати любі навантаження системи.

ВИСНОВОК

У рамках проекту комп'ютерного клубу "СКАЛА" була розроблена Кіберфізична система та комп'ютерна система з детальним втіленням корпоративної мережі, налаштуванням систем контролю та моніторингу мікроклімату та попередження про наявності клієнтов у залі. Після завершення проекту виявлено, що розроблена система в повній мірі відповідає всім вимогам, що ставились перед нами. Реалізація даного проекту передбачала аналіз об'єкту впровадження комп'ютерної системи, визначення технічних вимог, вибір мережевої архітектури, розробку специфікацій системного обладнання і комп'ютерної системи, розрахунок інтенсивності трафіку найбільшої підмережі, розробку адресації та логічної топології мережі, а також налаштування мережевого обладнання та захисту мережевих пристроїв від несанкціонованого доступу.

Крім того, було проведено аналіз трафіку та роботи систем за допомогою спеціалізованого програмного забезпечення для моделювання комп'ютерних мереж, а також розроблені системи контролю мікроклімату та моніторингу для забезпечєння загального комфорту в клубі як для клієнтів так і персоналу. Проект обґрунтовував важливість та необхідність впровадження сучасних технологій в установах розважальної галузі, зокрема в комп'ютерному клубі "СКАЛА".

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Методичні рекомендації довиконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123

2 Комп'ютернаінженерія Л.І.Цвіркун, С.М.Ткаченко, Я.В.Панферова, Д.О.Бешта, Л.В.Бешта. Д.:НТУ«ДП»,2023.–62с.

3 Iot for all (рекомендації) – [Електроннийресурс] – Режим доступу до ресурсу: https://www.iotforall.com/

4 CyberCafePro - Information on the latest hardware and software developments: https://cybercafepro.com

5 Мережа cisco – [Електроннийресурс] – Режим доступу до ресурсу:

6 https://www.cisco.com/site/us/en/products/networking/access-networking/index.html

7 Трой Макміллан « CiscoNetworkingEssentials» 2011.– 458 с

8 Майк Мейерс « CompTIA Network+ Certification » 2018. – 960 с

9 Европейский Центр Якості - https://www.centrumjakosci.pl/

10 ДСТУ 2860-94 Надійність техніки. Терміни та визначення.

11 ДСТУ 2862-94 Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги.

12 ДСТУ ISO/IEC 2382-14:2005 Інформаційні технології. Словник термінів. Частина 14. Безвідмовність, ремонтопридатність і готовність (ISO/IEC 2382-14:1997, IDT).

13 Пашков Е. В. Транспортно-нагромаджувальні і завантажувальні системи в складальному виробництві / Е. В. Пашков, В. Я. Копп, А. Г. Карлов. − К.: НМК ВО, 1992. − 520 с. − ISBN 577-6309-69-7