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 Чорненького Дмитра Ігоровича
(ПІБ)

академічної групи 123-21ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему «Комп'ютерна система ТОВ «ГРІН ФЬЮЧЕР ІНЖИНІРІНГ» з детальним опрацюванням побудови та налаштування корпоративної мережі та комплексу контроля мікроклімату в гідропонній теплиці»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Булана Т.М.			
спеціальної частини	доц. Булана Т.М.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.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 Чорненького Д.І **академічної групи** 123-21ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система ТОВ «ГРІН ФЬЮЧЕР ІНЖИНІРІНГ» з детальним опрацюванням побудови та налаштування корпоративної мережі та комплексу контроля живлення в мікроклімату теплиці»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 29.04.2024 № 375-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання побудови мережі компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ»	05.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними корпоративною мережею та системою комплексу контролю мікроклімату в гідропонній теплиці	12.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	26.05.2024
Розробка компонента системи	Розробити систему комплексу контролю мікроклімату в гідропонній теплиці	09.06.2024

Завдання видано _____ доц. Булана Т.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі 06.02.2024

Дата подання до екзаменаційної комісії 14.06.2024

Прийнято до виконання _____ Чорненький Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 67 с., 27 рис., 6 табл., 7 джерел.

КОМП’ЮТЕРНА СИСТЕМА, ІНТЕРНЕТ РЕЧЕЙ, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER, NAT, VPN, DHCP, VLAN.

Об’єкт розробки – Автоматизована система управління компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ», призначена для створення та конфігурації мережевої інфраструктури, що забезпечує комплексний моніторинг та контроль мікроклімату у гідропонній теплиці.

Мета роботи − створення комп’ютерної системи компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ».

Для компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ» була створена універсальна комп'ютерна мережа, здатна адаптуватися під різні потреби бізнесу завдяки гнучкому налаштуванню та перепрограмуванню.

Ця мережа спроєктована з урахуванням можливостей подальшого розширення та оновлення як апаратного, так і програмного забезпечення. Розробка цієї мережі стала результатом кваліфікаційної роботи бакалавра, виконаної згідно з поставленими завданнями.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ПК – персональний комп'ютер

СБД – система баз даних

UPS – джерело безперебійного живлення

AI – штучний інтелект

API – програмний інтерфейс додатків

DNS – система доменних імен

HTTP – протокол передачі гіпертексту

IoT – Інтернет речей

IP – Інтернет-протокол

ISP – Інтернет-провайдер

LAN – локальна обчислювальна мережа

SQL – мова структурованих запитів

UML – уніфікована мова моделювання

VLAN – віртуальна локальна мережа

VPN – віртуальна приватна мережа

WAN – глобальна обчислювальна мережа

°C – градус Цельсія

% – відсоток

ГБ (GB) – гігабайт

м² (m²) – квадратний метр

ВСТУП

У сучасному світі комп'ютерні технології є невід'ємною частиною успішного управління та контролю виробництва. Компанія «ГРІН ФЬЮЧЕР ІНЖИРІНГ», прагнучи досягти нових вершин продуктивності, обрала шлях інноваційного розвитку, впроваджуючи передові комп'ютерні системи у свою гідропонну теплицю.

Ключовим етапом цього масштабного проекту є створення комплексної системи контролю процесів живлення рослин. Вона охоплює всі аспекти виробництва, від розбудови мережевої інфраструктури до розробки інтелектуального програмного забезпечення для моніторингу та регулювання параметрів середовища в теплиці. Метою є досягнення максимальної ефективності та якості продукції.

У кваліфікаційній роботі детально розглянуто процес створення та налаштування мережі, що враховує специфічні потреби компанії. Крім того, робота описує розробку комплексної системи контролю, яка забезпечує ідеальні умови для росту рослин у гідропонній теплиці. Особливий акцент зроблено на надійності та безпеці системи, що досягається шляхом застосування передових технологій та дотримання найкращих практик у сфері інформаційної безпеки.

Зважаючи на динамічний розвиток технологій та зростаючі потреби компанії, система спроектована з урахуванням можливості її масштабування та подальшого вдосконалення. Ця робота є важливим кроком на шляху до оптимізації виробництва та зміцнення позицій компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ» на ринку.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи, що проектується.

Запропонована комп'ютерна система знаходить своє застосування в агрономії, зокрема, в автоматизації процесів вирощування рослин. Система призначена для створення та підтримки оптимальних умов для росту та розвитку рослин у контрольованому середовищі, а також для збору актуальних даних про їх стан. Вона інтегрується з автономними IoT-системами, які забезпечують самостійний контроль поливу, вентиляції, освітлення та інших важливих параметрів середовища, необхідних для здорового росту рослин.

Дана галузь охоплює кілька важливих напрямків. Першим є оптимізація умов вирощування рослин, що включає розробку систем контролю вологості, температури, освітлення та інших параметрів, які забезпечують оптимальний розвиток рослин. Це може включати використання гідропоніки, аеропоніки та інших методів безґрунтового вирощування.

Важливим напрямком є також дослідження та впровадження нових технологій у сільському господарстві. Це стосується використання інтернету речей (IoT), штучного інтелекту, дронів та інших передових інструментів для підвищення ефективності та продуктивності теплиць.

Генетичне вдосконалення рослин також є ключовим напрямком. Це включає створення нових сортів рослин, які є стійкими до шкідників, хвороб та несприятливих погодних умов, а також мають покращені смакові та якісні характеристики.

Ще одним важливим аспектом є розробка та впровадження екологічно чистих методів вирощування рослин. Ці методи не лише забезпечують високу врожайність, але й мінімізують негативний вплив на навколишнє середовище.

Нарешті, створення ефективних систем управління та моніторингу є невід'ємною частиною сучасного сільського господарства. Ці системи дозволяють швидко реагувати на зміни в умовах вирощування рослин та проводити аналіз для оптимізації процесів.

1.2 Характеристика і структура компанії «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ»

Компанія «ГРІН ФЬЮЧЕР ІНЖИРІНГ» є передовим підприємством у галузі сільського господарства, що спеціалізується на створенні та впровадженні автоматизованих систем для вирощування рослин у контрольованих умовах. Їх інноваційні рішення дозволяють ефективно використовувати ресурси, забезпечують високу якість продукції та мінімізують вплив на навколишнє середовище. Завдяки поєднанню передових технологій та експертного підходу, компанія гарантує своїм клієнтам надійність, ефективність та стабільність у процесі вирощування рослин.

«ГРІН ФЬЮЧЕР ІНЖИРІНГ» займається розробкою, виробництвом та реалізацією різноманітних продуктів для агросектору, включаючи освітлювальні системи, блоки контролю та управління автоматичним поливом, спеціалізовані світлодіодні фіто-світильники, стелажні гідропонні системи, а також комплектуючі, що сприяють швидкому росту, розвитку та дозріванню різних рослин, включаючи живці та розсаду.

Виробничі потужності компанії дозволяють створювати фіто-світильники та складні гідропонні системи, починаючи від етапу розробки та практичних досліджень, і завершуючи випуском готової продукції під ключ.

1. Науково-дослідний підрозділ є рушійною силою інновацій у компанії, відповідаючи за створення та вдосконалення технологій та продуктів. Інженери та дослідники цього центру працюють над новими методами вирощування рослин, проводять випробування та впроваджують передові рішення.

2. Виробничий відділ зосереджує процеси виробництва та збирання автоматизованих систем. Висококваліфіковані робітники та інженери-технологи забезпечують бездоганну якість продукції, що випускається компанією.

3. Комерційний департамент відповідає за просування продукції на ринку, залучення нових клієнтів та підтримку зв'язків з існуючими. Менеджери з продажу, маркетологи та фахівці з реклами та PR працюють разом, щоб забезпечити успішний збут продукції.

4. Фінансовий департамент здійснює фінансове планування, облік та контроль фінансових операцій компанії. Бухгалтери, фінансові аналітики та менеджери забезпечують ефективне управління фінансовими ресурсами компанії.

5. Департамент управління персоналом та адміністративної підтримки відповідає за управління кадрами, розвиток персоналу та загальне адміністрування офісу. Менеджери з персоналу, HR-фахівці, адміністратори та офіс-менеджери забезпечують ефективну роботу команди та комфортне робоче середовище.

Рисунок 1.1 – Схема організаційної структури компанії «Green Future»

1.3 Стислі відомості про топологічне розміщення структурних підрозділів компанії «ГРІН ФЬЮЧЕР»

Усі структурні підрозділи компанії розташовані в одному приміщенні – офісі, що займає третій поверх нежитлової будівлі за адресою: просп. Лесі Українки, 21, м. Дніпро, Дніпропетровська область, 49000. Офіс складається з п'яти кімнат.(рис 1.).

Топографічна схема розміщення структурних підрозділів показана на рис. 1.2

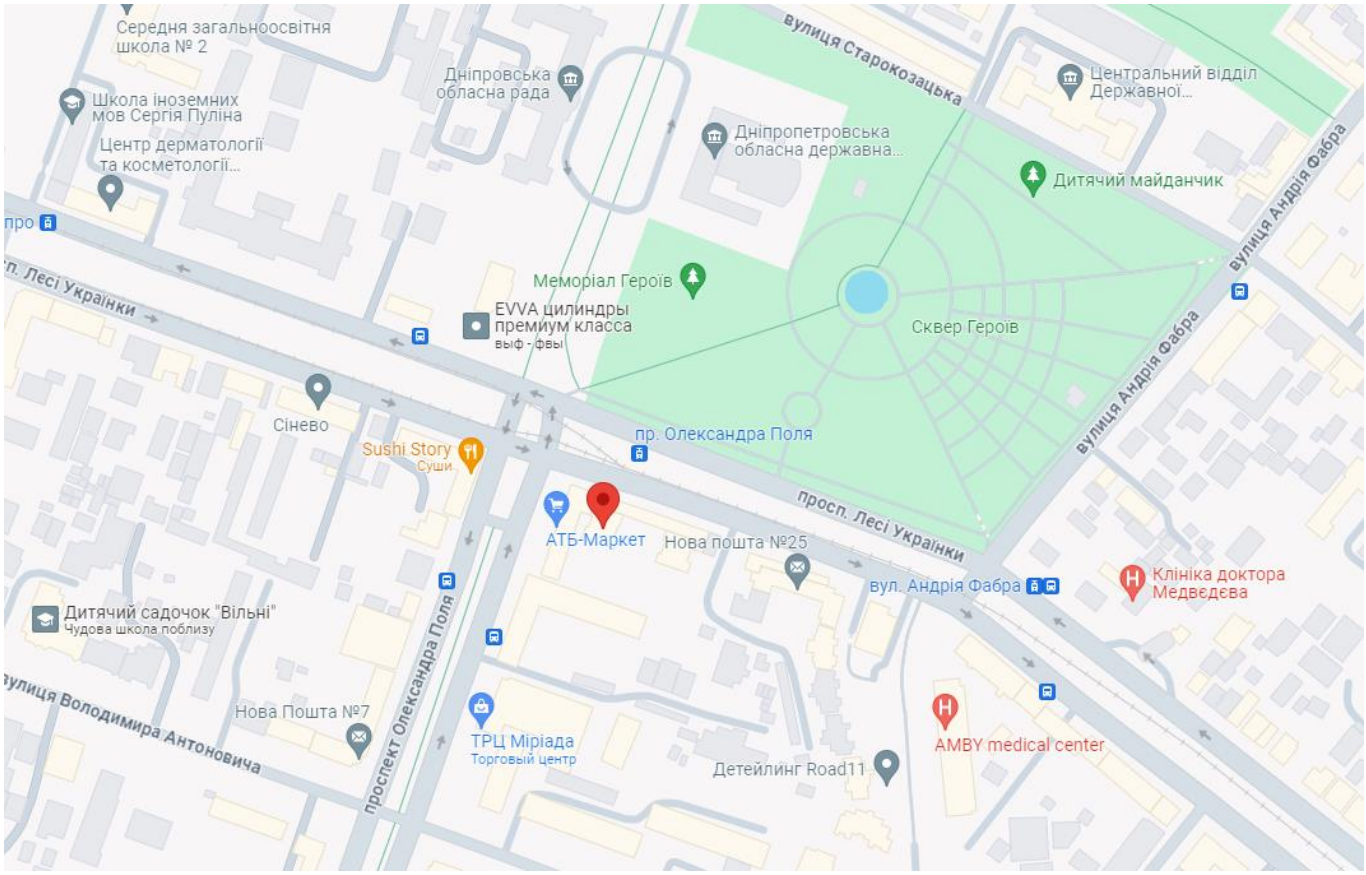

Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів компанії «Green Future»

Структурна схема розміщення підрозділів у будівлі включає такі відділи: фінансовий, продажів та маркетингу, адміністративний та кадровий, досліджень та розробок, а також зону для тестування та досліджень.(рис. 1.3).

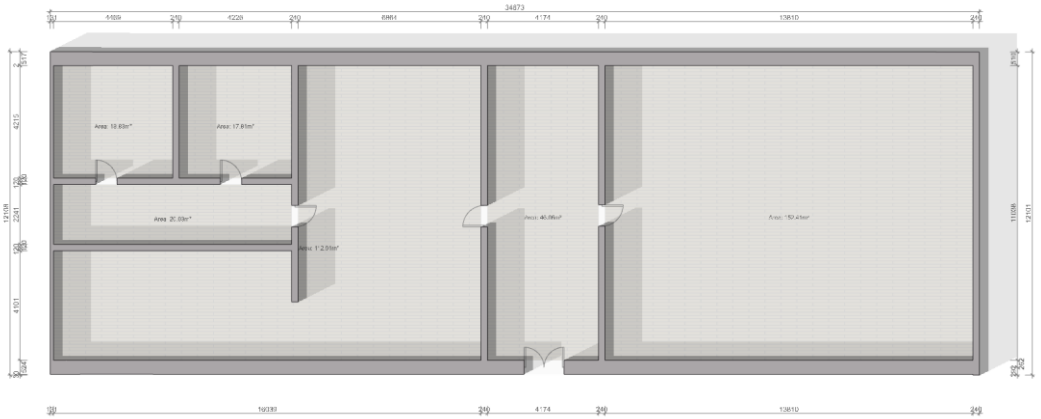

Рисунок 1.3 – Структурна схема розміщення підрозділів у будівлі

1.4 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

У сучасному сільському господарстві існує безліч технологічних рішень, які постійно розвиваються та вдосконалюються, забезпечуючи інформаційну підтримку процесів вирощування рослин.

– Автоматизація процесів вирощування дозволяє оптимізувати та стабілізувати умови в гідропонних системах завдяки застосуванню автоматичних систем поливу, дозування поживних речовин, регулювання вологості та освітлення.

– Використання датчиків та сенсорів для вимірювання температури, вологості, рівня pH та інших параметрів дозволяє здійснювати безперервний моніторинг умов вирощування та автоматично реагувати на будь-які зміни.

– Системи автоматичного керування, що базуються на мікроконтролерах або комп'ютерних системах, дозволяють програмувати та керувати процесами в гідропонній системі на основі даних, отриманих від датчиків та сенсорів.

– Системи моніторингу та аналізу даних забезпечують збір, аналіз та візуалізацію інформації, що дозволяє оперативно контролювати стан системи, виявляти відхилення від норми та вживати відповідних заходів.

– Системи віддаленого керування надають можливість керувати гідропонними системами через Інтернет або мобільний додаток, що забезпечує зручність та доступність для операторів з будь-якого місця.

– Безпека та захист даних є важливим аспектом, який забезпечується за допомогою шифрування, автентифікації та інших заходів безпеки, що захищають гідропонні системи від несанкціонованого доступу та втрати інформації.

– Надійно спроектована та захищена мережева інфраструктура є основою для ефективної та безпечної роботи всіх цих систем.

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

Для ефективної обробки та передачі інформації в гідропонних системах важливо використовувати надійні та масштабовані технології. Сучасні рішення Інтернету речей (IoT) дозволяють збирати дані з різних датчиків у режимі реального часу та забезпечувати їхню швидку обробку та передачу для подальшого аналізу та управління.

Такі системи зазвичай включають:

– спеціалізовані протоколи передачі даних, такі як MQTT або CoAP, які оптимізовані для мінімізації навантаження на мережу та забезпечення високої надійності в IoT-застосунках.

– Хмарні платформи, такі як AWS IoT Core або Microsoft Azure IoT Hub, що надають потужні інструменти для обробки, зберігання та аналізу даних.

– Edge Computing, що дозволяє здійснювати попередню обробку даних безпосередньо на пристроях, зменшуючи час реакції та обсяг даних, що передаються через мережу.

Архітектура об'єкта впровадження включає рішення, що забезпечують гнучкість, масштабованість та інтеграцію системи. Основні принципи включають:

– Модульність, що дозволяє легко розширювати або змінювати систему.

– Стандартизацію компонентів для забезпечення їх взаємозамінності та сумісності.

– Автоматизацію процесів для підвищення ефективності та мінімізації впливу людського фактору.

Відомі рішення в цій галузі включають технології та платформи, які успішно застосовують подібні системи в аналогічних умовах. Прикладами є:

– Контрольні системи від таких компаній, як Hoogendoorn та Priva, що пропонують комплексні рішення для автоматизації та управління сільськогосподарськими теплицями.

– Розумні агротехнології, розроблені компаніями AgriTech, які зосереджені на оптимізації виробництва за допомогою автоматизованого контролю клімату та живлення рослин.

Аналіз існуючих методів обробки та передачі інформації для корпоративної мережі ТОВ "ГРІН ФЬЮЧЕР ІНЖИНІРИНГ":

Ключовими технологіями для обробки та передачі інформації є ті, що забезпечують швидкість, безпеку та стабільність мережевих операцій:

– Ethernet та Wi-Fi: Основні технології для фізичного підключення в корпоративних мережах. Ethernet використовується для створення надійних провідних мереж з високою пропускною здатністю, тоді як Wi-Fi забезпечує гнучкий бездротовий доступ.

– MPLS (Multiprotocol Label Switching): Технологія, що підвищує ефективність передачі даних шляхом створення віртуальних шляхів між джерелом та приймачем.

– VPN (Virtual Private Network): Забезпечує безпечне з'єднання між користувачами та корпоративними ресурсами через Інтернет шляхом шифрування всіх переданих даних.

Принципи побудови корпоративних мереж включають:

– Масштабованість та адаптивність: Мережа повинна бути спроектована так, щоб легко пристосовуватися до змін у кількості користувачів або вимогах до ресурсів без необхідності кардинальних переробок.

– Надійність та відновлюваність: Забезпечення високої доступності та мінімізації часу простою шляхом впровадження резервних каналів зв'язку та систем відновлення після збоїв.

– Безпека: Використання сучасних заходів безпеки, таких як брандмауери, системи виявлення вторгнень (IDS) та шифрування даних для захисту від зовнішніх та внутрішніх загроз.

На ринку представлено багато надійних рішень та продуктів від провідних виробників, які використовуються для побудови ефективних корпоративних мереж:

– Cisco Systems: Один з лідерів у галузі мережевого обладнання, що пропонує широкий спектр рішень - від комутаторів та маршрутизаторів до комплексних систем безпеки.

– Juniper Networks: Компанія відома своїми високопродуктивними мережевими рішеннями, особливо в сфері маршрутизації та захисту даних.

– HP Enterprise: Постачає широкий асортимент мережевого обладнання, включаючи комутатори, маршрутизатори та технології бездротового зв'язку.

1.6 Завдання і мета роботи

Метою цієї роботи є розробка комплексної комп'ютерної системи для ТОВ «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ», яка включатиме детальне проектування та налаштування корпоративної мережі, а також системи контролю процесів живлення в гідропонній теплиці.

Для досягнення поставленої мети необхідно виконати наступні кроки:

– Вивчити особливості та потреби компанії «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ» для визначення оптимальних рішень;

– Визначити конкретні технічні параметри та характеристики, яким повинна відповідати майбутня система;

– Вибрати найбільш підходящу мережеву архітектуру та обладнання, що відповідають потребам компанії та забезпечують ефективну роботу системи;

– Детально описати технічні характеристики та вимоги до всіх апаратних компонентів системи;

– Вивчити обсяги та характер мережевого трафіку для оптимізації роботи системи та забезпечення її пропускної здатності;

– Створити детальну модель мережі та налаштувати всі її компоненти для забезпечення безперебійної та ефективної роботи;

– Створити систему, яка забезпечуватиме автоматичний контроль та управління процесами живлення рослин у гідропонній теплиці;

– Перевірити працездатність мережі в цілому та кожного її компонента окремо для виявлення та усунення можливих помилок та недоліків.

Результатом роботи повинна бути масштабована, надійна та безпечна мережа, а також комплекс контролю процесів живлення в гідропонній теплиці, що відповідає всім вимогам та потребам компанії «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ».

1.7 Визначення можливих напрямків рішення завдань

Розробка архітектури мережі передбачає:

– Ключова мета: Створення адаптивної та масштабованої мережевої архітектури, здатної ефективно справлятися зі зростанням обсягів даних та кількості мережевих пристроїв.

– Впровадження передових технологій: Використання сучасних стандартів Ethernet та Wi-Fi для забезпечення швидкої та надійної передачі даних.

– Забезпечення безпеки: Застосування віртуальних приватних мереж (VPN) для захищеного підключення до віддалених ресурсів.

– Оптимізація маршрутизації: Інтеграція технології MPLS для підвищення ефективності управління мережевим трафіком у корпоративній мережі.

Вибір та інтеграція обладнання:

– Ключова мета: Підбір оптимального мережевого обладнання, яке відповідає технічним вимогам проекту.

– Підбір компонентів: Вибір мережевих комутаторів та маршрутизаторів, що забезпечують необхідну пропускну здатність та рівень безпеки.

– Зберігання даних: Розгляд варіантів мережевого сховища даних для ефективного архівування та швидкого доступу до інформації.

– Забезпечення безперервної роботи: Впровадження резервних систем для гарантування високої доступності мережевих ресурсів.

Безпека мережі:

– Ключова мета: Забезпечення високого рівня безпеки даних та мережевих операцій.

– Комплексний підхід: Розробка всебічної стратегії безпеки, що включає брандмауери, антивірусне програмне забезпечення та інші інструменти кібербезпеки.

– Активний захист: Впровадження систем виявлення та запобігання вторгненням для моніторингу та оперативного реагування на потенційні загрози.

– Конфіденційність даних: Застосування шифрування для захисту чутливої інформації, що передається мережею.

Моніторинг та адміністрування мережі:

– Ключова мета: Створення системи моніторингу, яка забезпечить швидке виявлення та ефективне усунення проблем у мережі.

– Контроль стану: Впровадження інструментів моніторингу, що надають детальну інформацію про роботу мережевих компонентів та характеристики трафіку.

– Підтримка працездатності: Розробка політик адміністрування, що включають регулярне оновлення програмного забезпечення та апаратних компонентів для забезпечення безперебійної роботи мережі.

Розробка та інтеграція системи контролю процесів живлення:

– Ключова мета: Впровадження передових технологій для контролю та автоматизації процесів у гідропонній теплиці.

– Інтеграція IoT: Використання рішень Інтернету речей для збору даних з датчиків та автоматичного регулювання умов вирощування рослин.

– Програмне забезпечення: Розробка програмного забезпечення для управління та аналізу отриманих даних, що дозволить оптимізувати використання ресурсів та підвищити продуктивність теплиці.

Кожен з цих напрямків потребує ретельного планування та реалізації з урахуванням специфічних потреб та умов компанії «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ», щоб забезпечити успішне впровадження та ефективну експлуатацію розробленої системи.

1.8 Обґрунтування вибраного напрямку інженерного рішення

Вибір інженерного рішення для комп'ютерної системи компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ» базується на детальному аналізі вимог до функціональності, надійності та продуктивності, з урахуванням особливостей діяльності компанії та експлуатаційних умов.

В першу чергу, були визначені основні вимоги до системи: висока продуктивність, надійність, безпека та масштабованість. Система повинна забезпечувати безперервну роботу гідропонної теплиці, що вимагає постійного контролю та управління численними параметрами мікроклімату, такими як температура, вологість, освітлення тощо.

Компанія «ГРІН ФЬЮЧЕР ІНЖИРІНГ» спеціалізується на розробці передових рішень для аграрного сектору, що вимагає застосування сучасних технологій та високого рівня автоматизації. Це обумовлює необхідність інтеграції кіберфізичних систем з комп'ютерними мережами, забезпечення зручного доступу до даних та можливості оперативного реагування на зміни умов.

З огляду на аналіз вимог та специфіки діяльності компанії, було прийнято рішення використовувати мікроконтролери Arduino та Raspberry Pi Pico для збору даних та управління процесами в теплиці. Ці платформи дозволяють легко інтегрувати різноманітні датчики та виконавчі механізми, забезпечуючи гнучкість та можливість швидкої адаптації системи до нових вимог.

Для ефективного управління та обміну даними між компонентами системи було обрано трирівневу архітектуру: ядро, доступ та хости. Це забезпечує високу пропускну здатність, надійність та легкість масштабування мережі. Використання маршрутизаторів та комутаторів з підтримкою VLAN та резервування гарантує стабільність та безпеку мережевих з'єднань.

Важливим аспектом є вибір енергоефективних компонентів для зниження експлуатаційних витрат та забезпечення екологічної стійкості. Застосування сучасних енергоефективних мікроконтролерів та мережевого обладнання дозволяє досягти оптимального балансу між продуктивністю та енергоспоживанням.

Обране інженерне рішення базується на інтеграції сучасних технологій у сфері комп'ютерної інженерії та кіберфізичних систем, що дозволяє створити продуктивну, надійну та масштабовану систему управління гідропонною теплицею. Такий підхід забезпечує високий рівень автоматизації, захист даних та можливість подальшого розвитку і модернізації системи відповідно до потреб компанії.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ АБО КІБЕРФІЗИЧНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп’ютерної системи компанії та кіберфізичної системи

2.1.1 Вимоги до систем в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

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

Спроектована комп'ютерна система призначена для забезпечення безперебійного обміну інформацією та управління компанією «ГРІН ФЬЮЧЕР ІНЖИНІРИНГ», включаючи підтримку досліджень за допомогою кіберфізичної системи.

Для реалізації цього проекту необхідно створити п'ять локальних мереж, використовуючи IP-адреси для призначення підмереж.

Корпоративна мережа компанії повинна складатися з наступних п'яти підмереж:

– фінансовий відділ;

– відділ продажів та маркетингу;

– відділ адміністрування та кадрів;

– відділ досліджень та розробок;

– віддалена мережа.

Відповідно до загальної архітектури, корпоративна мережа компанії буде розділена на локальні мережі (системи).

Розділення на п’ять підмереж надає певні переваги, а саме:

– спрощене адміністрування. Розподіл мережі на підмережі полегшує її управління для мережевих адміністраторів.

– Підвищена продуктивність. Розділення дозволяє забезпечити високу швидкість передачі даних у кожній локальній підмережі.

– Масштабованість. Така структура мережі дозволяє легко додавати або замінювати пристрої в локальних підмережах без впливу на інші частини мережі.

– Покращена безпека. Розподіл на підмережі дозволяє впровадити точніші системи безпеки, такі як брандмауери або VPN, для захисту кожної підмережі окремо.

Необхідно розділити IP-адресу 172.24.200.0/21 на 5 підмереж, забезпечуючи можливість збільшення кількості вузлів у кожній підмережі з урахуванням планів замовника щодо розширення компанії. Також необхідно налаштувати взаємодію цих підмереж з локальними серверами компанії в рамках локальної мережі (LAN), враховуючи наступну кількість вузлів у кожній підмережі:

– підмережа LAN_1 – забезпечує 5 вузлів, технологію EtherChannel;

– підмережа LAN_2 – забезпечує 101 вузлів;

– підмережа LAN_3 – забезпечує 208 вузлів, технологію VLAN;

– підмережа LAN_4 – забезпечує 85 вузлів;

– підмережа LAN_5 – забезпечує 5 вузлів.

Створення кіберфізичної системи управління освітленням та температурою є наступним етапом після розробки мережевої інфраструктури. Система забезпечуватиме точне управління інтенсивністю освітлення за допомогою світлодіодних фіто-світильників, а також підтримуватиме ідеальний температурний режим, використовуючи системи обігріву та вентиляції.

Система буде постійно відстежувати та аналізувати наступні параметри:

– рівень освітленості;

– спектральний склад світла;

– температуру повітря в теплиці;

– температуру субстрату (за наявності).

2.1.1.1.2 Вимоги до характеристик взаємозв’язків створюваної системи із суміжними системами

Для обміну інформацією між вузлами використовується технологія Ethernet та протокол маршрутизації OSPF. Взаємодія між вузлами кіберфізичних систем забезпечується налаштованим IoT-сервером та каналами передачі даних, такими як Ethernet або Wi-Fi.

2.1.1.1.3 Вимоги до режимів функціонування систем

Безперервна працездатність.Система повинна гарантувати стабільний доступ до ключових функцій, таких як збереження даних та управління кіберфізичними системами, навіть у випадку тимчасових збоїв або відмов обладнання.

Швидке відновлення.У разі виникнення неполадок система повинна мати можливість швидко та ефективно відновити нормальний режим роботи, мінімізуючи вплив на продуктивність.

Адаптивність.Система має бути гнучкою та здатною до розширення функціоналу шляхом додавання нових компонентів або модернізації обладнання.

Надійний захист.Різні режими роботи системи повинні забезпечувати високий рівень безпеки та захисту від несанкціонованого доступу.

Масштабованість.Система повинна мати можливість розширюватися відповідно до зростаючих потреб користувачів та обсягів даних, не втрачаючи при цьому продуктивності.

2.1.1.1.4 Вимоги до діагностування системи

Співробітники повинні мати можливість самостійно виявляти потенційні проблеми та несправності в роботі системи, аналізуючи доступну інформацію та спостерігаючи за її функціонуванням.

Для своєчасного виявлення проблем працівники повинні регулярно перевіряти стан компонентів, ресурсів та процесів системи. Це здійснюється шляхом аналізу даних, отриманих з датчиків, а також врахуванням відгуків та скарг працівників щодо роботи мережі.

2.1.1.1.5 Перспективи розвитку, модернізації системи

Вимоги до комп’ютерної системи

Масштабованість:

Впровадження новітніх технологій захисту інформації, обліку та протоколів передачі даних має бути здійснено з фокусом на адаптивність інфраструктури.

Система має бути спроектована з урахуванням майбутнього зростання компанії, використовуючи мережеві архітектури, віртуалізацію та хмарні технології для забезпечення легкого розширення ресурсів.

Інноваційність:

Система повинна підтримувати інтеграцію передових технологій, таких як штучний інтелект, машинне навчання та Інтернет речей (IoT), для оптимізації процесів та підвищення ефективності.

Гнучкість та надійність:

Система має бути гнучкою, надійною та готовою до інтеграції з новими технологіями, що забезпечить конкурентоспроможність компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ» на ринку.

Вимоги до кіберфізичної системи

Модульність:

Кіберфізична система гідропонної теплиці повинна мати модульну структуру, що дозволить швидко замінювати компоненти у разі їх пошкодження або необхідності модернізації.

Модульність також має забезпечити можливість додавання нових функціональних блоків без суттєвих змін у загальній архітектурі системи.

Інтеграція нових технологій:

Використання IoT-датчиків для моніторингу стану рослин та умов навколишнього середовища дозволить своєчасно виявляти проблеми та приймати оптимальні рішення для їх вирішення.

Програмне забезпечення:

Програмне забезпечення системи має бути розроблене на основі гнучкої та сучасної мови програмування, такої як microPython, що забезпечить високу

ефективність розробки, підтримки та спрощення процесу інтеграції нових функцій та технологій.

2.1.1.2 Вимоги до показників призначення

Система повинна відповідати наступним вимогам:

– ефективна комунікація. Забезпечення співробітників інструментами для швидкого обміну інформацією, такими як месенджери, електронна пошта та відеоконференції.

– Обмін даними та спільний доступ. Надання працівникам можливості отримувати дані з кіберфізичних систем та обмінюватися корпоративною інформацією між різними пристроями.

– Централізоване та резервне зберігання даних. Забезпечення централізованого зберігання даних на серверах компанії з можливістю резервного копіювання в хмару для захисту від втрати інформації.

– Надійна безпека. Впровадження комплексних механізмів безпеки для захисту даних від несанкціонованого доступу та шкідливого програмного забезпечення.

– Доступ до Інтернету. Надання всім співробітникам можливості підключатися до глобальної мережі Інтернет.

– Віддалений доступ. Забезпечення можливості безпечного віддаленого підключення до корпоративної мережі через VPN.

2.1.1.3 Вимоги до патентної чистоти

Для забезпечення відповідності патентним вимогам, обладнання та програмне забезпечення, що використовується в комп'ютерній системі, повинно бути ретельно перевірено. Це включає використання лише ліцензійного програмного забезпечення, проведення детального аналізу компонентів системи на наявність можливих патентів та отримання юридичних консультацій щодо цього питання. Крім того, важливо вести детальну документацію процесу проектування

компонентів системи, щоб у разі виникнення претензій від виробників мати докази патентної чистоти розробки.

Для мінімізації ризиків, пов'язаних з патентними порушеннями, необхідно постійно відстежувати зміни в патентному законодавстві та базах патентів. Це передбачає регулярний моніторинг нових патентних заявок, аналіз патентних спорів та відстеження діяльності конкурентів у цій сфері. Такий підхід допоможе вчасно виявити потенційні ризики та уникнути фінансових та юридичних наслідків.

Важливим аспектом є також співпраця з розробниками та постачальниками обладнання і програмного забезпечення для забезпечення патентної чистоти. Усі контракти з постачальниками повинні містити положення щодо дотримання патентних прав та захисту від можливих претензій третіх осіб. Це не тільки захистить компанію від потенційних патентних суперечок, але й забезпечить стабільну та безперебійну роботу комп'ютерної системи та її компонентів у довгостроковій перспективі.

2.1.1.4 Додаткові вимоги

Система повинна бути адаптована до роботи в умовах гідропонної теплиці, тобто витримувати широкий діапазон температур та вологості. Обладнання має бути захищене від пилу, вологи та механічних пошкоджень, а також забезпечувати захист від електромагнітних перешкод.

Вимоги до активного обладнання:

Безперебійна робота: Обладнання має забезпечувати стабільну та безперервну роботу системи 24/7. Маршрутизатори та комутатори повинні підтримувати необхідні протоколи та стандарти для ефективного обміну даними.

Достатність портів з резервом: Маршрутизатори повинні мати не менше 3 портів GigabitEthernet, а комутатори – 24 порти FastEthernet та один порт GigabitEthernet. Кількість портів має бути достатньою для можливого розширення системи в майбутньому.

Монтаж: Обладнання має бути встановлене у відповідні комутаційні шафи.

Технічні характеристики: Активне обладнання повинно бути енергоефективним, мати низький рівень шуму та забезпечувати легкий доступ для технічного обслуговування та ремонту.

Вимоги до кабель-каналів, інформаційних та електричних розеток:

Матеріал та розміри: Кабель-канали повинні бути виготовлені з негорючих матеріалів та мати достатній розмір для прокладання кабелів з урахуванням їхнього можливого розширення.

Розміщення: Кабель-канали та розетки повинні бути розміщені зручно для підключення обладнання та забезпечувати легкий доступ для технічного обслуговування при модернізації або заміні/додаванні компонентів.

Вимоги до комунікаційного обладнання та його розташування:

Розміщення: Комунікаційне обладнання має бути розміщене у спеціально відведених приміщеннях з контрольованими умовами температури та вологості.

Тип шаф: Використовувати серверні шафи стандарту 19 дюймів, що забезпечують належний рівень вентиляції та доступу для обслуговування.

Підведення кабельних трас: Кабельні траси повинні бути прокладені з урахуванням можливості їх розширення (приблизно на 30-40%), використовуючи стандартизовані кріплення та захисні канали.

Розташування обладнання в шафі: Обладнання повинно бути розміщене таким чином, щоб забезпечити оптимальний повітряний потік для охолодження та легкий доступ до кабельних з'єднань.

Вимоги до однорідності:

Стандартизація: Система повинна використовувати однорідні типи кабелів, роз'ємів та магістралей для забезпечення сумісності та зниження витрат на технічне обслуговування. Це включає використання стандартних категорій Ethernet-кабелів (наприклад, Cat5e або Cat6), однакових типів роз'ємів (RJ45) та кабельних трас.

Вимоги до резервування:

Дублювання: Система повинна мати резервні копії критичних компонентів, включаючи резервні канали зв'язку, дублюючі маршрутизатори та комутатори, а

також джерела безперебійного живлення (UPS) для забезпечення безперервної роботи у разі відмови основних компонентів.

Спеціальні вимоги:

Резервне копіювання: Повинні бути передбачені механізми для регулярного резервного копіювання даних та швидкого відновлення у разі втрати інформації.

Безпека: Система повинна відповідати вимогам інформаційної безпеки, включаючи використання шифрування даних, авторизації та аутентифікації користувачів, а також засобів захисту від кіберзагроз.

Інтеграція: Повинна бути забезпечена сумісність та можливість інтеграції з існуючими інформаційними системами компанії для забезпечення безперервності бізнес-процесів.

2.1.2 Вимоги функцій, виконуваним системою

Вимоги до функцій комп'ютерної системи:

Комп'ютерна система повинна забезпечувати:

– Ефективне управління мережею: моніторинг та контроль мережевого трафіку, забезпечення безпеки мережі, управління підключеннями та доступом.

– Надійне управління даними: зберігання, обробка та резервне копіювання даних, управління базами даних, забезпечення цілісності та доступності даних.

– Якісну підтримку користувачів: управління обліковими записами користувачів, надання технічної підтримки, забезпечення доступу до корпоративних ресурсів.

– Потужну аналітику та звітність: збір, обробка та аналіз даних, генерація звітів та аналітичних довідок для прийняття обґрунтованих рішень.

Часовий регламент та вимоги до якості:

– Управління мережею: затримка передачі даних не повинна перевищувати 50 мс, доступність мережі – 99.9%.

– Управління даними: резервне копіювання повинно виконуватися щоденно, час відновлення даних – не більше 2 годин, цілісність даних – 100%.

– Підтримка користувачів: час реакції на запити користувачів – не більше 1 години, вирішення проблем – не більше 24 годин.

– Аналітика та звітність: звіти повинні генеруватися щотижня, точність даних – 99%, час виконання аналітичних запитів – не більше 30 хвилин.

Вимоги до функцій кіберфізичної системи:

Кіберфізична система повинна забезпечувати:

– Точний моніторинг середовища: збір даних з датчиків температури, вологості, освітленості та інших параметрів.

– Автоматизоване управління процесами: керування системами поливу, освітлення, вентиляції та живлення на основі зібраних даних.

– Аналіз та прогнозування: обробка даних для виявлення тенденцій та аномалій, прогнозування потреб рослин у ресурсах.

– Швидке аварійне реагування: виявлення та реагування на критичні ситуації, такі як перевищення допустимих рівнів температури або вологості.

Часовий регламент та вимоги до якості:

– Моніторинг середовища: збір даних кожні 5 хвилин, точність вимірювань – ±2% для температури, ±5% для вологості.

– Управління процесами: реакція на зміни параметрів середовища не більше 1 хвилини, доступність системи управління – 99.9%.

– Аналіз і прогнозування: оновлення прогнозів кожні 24 години, точність прогнозів – 95%.

– Аварійне реагування: час реагування на аварійну ситуацію – не більше 30 секунд, точність виявлення критичних ситуацій – 99%.

–

2.1.3 Вимоги до видів забезпечення комп’ютерної системи

Для забезпечення безперебійної та точної роботи системи важливо врахувати декілька аспектів математичного забезпечення. По-перше, необхідно забезпечити точне перетворення даних з датчиків температури (DS18B20 і DHT11) у градуси Цельсія. Це включає калібрування датчиків та обробку можливих похибок вимірювання. Для DS18B20 використовується метод read_temp(), який

безпосередньо повертає температуру в градусах Цельсія. Для DHT11 необхідно враховувати можливі похибки у вимірюванні вологості та температури, що може потребувати додаткової обробки результатів.

По-друге, код передбачає роботу з аналоговими датчиками, такими як датчики рівня води та pH. Для кожного з них важливо забезпечити точне аналогово-цифрове перетворення (ADC).

Нарешті, для забезпечення стабільного мережевого підключення та передачі даних на сервер використовується Wi-Fi модуль. Необхідно забезпечити надійне підключення до мережі та коректну передачу даних, включаючи обробку можливих помилок з'єднання або втрати даних. Це включає розробку відповідного протоколу передачі даних, який використовує структуровані пакети для відправки множинних вимірювань на сервер, а також обробку з'єднань та відновлення у випадку збоїв. Оскільки підключення до мережі може бути нестабільним, важливо передбачити механізми повторного підключення та перевірки успішності передачі даних.

2.1.3.1 Вимоги до інформаційного забезпечення

Вимоги до комп'ютерної системи:

– організація даних. Чітка, структурована організація даних, що включає всі необхідні елементи для ефективної роботи. Використання уніфікованих форматів та стандартів забезпечить узгодженість та цілісність інформації.

– Обмін інформацією. Швидкий та надійний обмін даними між компонентами системи. Для цього потрібно впровадити ефективні протоколи передачі даних та механізми синхронізації між різними модулями системи.

– Сумісність. Комп'ютерна система повинна бути сумісною з іншими системами компанії, підтримуючи стандарти обміну даними, інтегруючись з наявним програмним та апаратним забезпеченням, та забезпечуючи безперешкодний обмін інформацією з зовнішніми системами.

– Системи керування базами даних (СКБД). Використання надійних СКБД для ефективного зберігання та обробки даних. Вибір СКБД повинен відповідати вимогам до швидкості доступу, обсягу даних та безпеки інформації.

Вимоги до кіберфізичної системи:

– Структура процесів. Чітко визначені та структуровані процеси збору, обробки та передачі даних. Використання датчиків для збору даних, алгоритмів для їх обробки та надійних каналів передачі інформації до центральної системи управління.

– Контроль та збереження даних. Забезпечення контролю за збереженням даних та можливість їх відновлення у разі втрати або пошкодження. Впровадження механізмів резервного копіювання, моніторингу стану системи та протоколів відновлення інформації.

– Обмін інформацією. Безперервний та ефективний обмін інформацією між компонентами системи. Використання стандартних протоколів передачі даних та забезпечення надійності та безпеки цих процесів.

– Сумісність. Кіберфізична система повинна бути сумісною з іншими інформаційними та технічними системами теплиці та компанії. Це забезпечить інтегроване управління всіма процесами та підвищить ефективність роботи системи.

2.1.3.2 Вимоги до лінгвистичного забезпечення

Вимоги до мов програмування:

Для забезпечення ефективності та зручності підтримки програмного забезпечення системи, необхідно використовувати мови програмування високого рівня, такі як Python, C++ або Java. Ці мови відрізняються високою продуктивністю, зрозумілим синтаксисом та широкою підтримкою спільноти розробників.

Вимоги до мов взаємодії користувачів та технічних засобів:

Інтерфейс користувача повинен бути розроблений з використанням мов, що забезпечують інтуїтивну та зручну взаємодію з системою. Для веб-застосунків рекомендується використовувати HTML, CSS та JavaScript, а для десктопних застосунків – відповідні мови, такі як C# для Windows Forms або WPF.

Для забезпечення ефективної взаємодії між технічними компонентами системи (датчиками, контролерами тощо) необхідно використовувати стандартизовані протоколи та мови, такі як MQTT, HTTP або Modbus, які гарантують надійний обмін даними.

Вимоги до кодування та декодування даних:

Для забезпечення сумісності між різними компонентами системи необхідно використовувати стандартизовані методи кодування та декодування даних. Рекомендується використовувати формати JSON або XML для обміну даними, а також базові методи кодування, такі як Base64, для передачі бінарних даних через текстові протоколи.

Вимоги до мов маніпулювання даними:

Для обробки та маніпулювання даними в системі слід використовувати мови, що забезпечують ефективну роботу з базами даних та іншими джерелами інформації. Для реляційних баз даних основною мовою є SQL, тоді як для NoSQL баз даних можна використовувати відповідні API та запити на базі JavaScript (наприклад, для MongoDB).

Вимоги до засобів опису предметної області:

Для опису об'єкта автоматизації (предметної області) необхідно використовувати спеціалізовані мови та нотації, такі як UML (Unified Modeling Language), які дозволяють візуально моделювати та зрозуміло описувати структуру та поведінку системи.

Вимоги до способів організації діалогу:

Для забезпечення ефективної взаємодії користувача з системою слід використовувати сучасні методи організації діалогу, такі як інтерактивні вікна, асистенти на базі штучного інтелекту, підказки та повідомлення про помилки. Інтерфейси повинні бути розроблені з урахуванням принципів юзабіліті та

доступності, щоб забезпечити максимально зручне користування системою для всіх категорій користувачів.

2.1.3.3 Вимоги до безпеки корпоративної мережі

Вимоги до робочих місць:

Кожне робоче місце має бути оснащене комп'ютером з чотириядерним процесором (або більше) з тактовою частотою від 2 ГГц, не менше 8 ГБ оперативної пам'яті, дискретним відеоадаптером та накопичувачем об'ємом від 256 ГБ. Операційна система - Windows 10 або Windows 11.

Вимоги до сервера:

Сервер повинен мати процесор з тактовою частотою від 1,5 ГГц та не менше 8 ГБ оперативної пам'яті.

Вимоги до комутатора:

Комутатор повинен мати 24 порти FastEthernet, порт GigabitEthernet та підтримувати технології Etherchannel та VLAN.

Вимоги до маршрутизатора:

Маршрутизатор повинен мати мінімум 3 порти GigabitEthernet, 4 слоти EHWIC та підтримувати DHCP, NAT, VPN та модель AAA.

Вимоги до кіберфізичної системи:

Кіберфізична система, що базується на Arduino або Raspberry Pi Pico, повинна відповідати наступним вимогам:

Мікроконтролери:

– Arduino: моделі з достатньою кількістю входів/виходів для підключення датчиків та виконавчих механізмів (наприклад, Arduino Uno, Arduino Mega).

– Raspberry Pi Pico: двоядерний процесор ARM Cortex-M0+, 264 КБ SRAM, 2 МБ флеш-пам'яті, підтримка PIO.

Датчики:

– Температури та вологості: точні та енергоефективні.

– Освітленості: для моніторингу рівня освітлення.

– Рівня pH: для контролю кислотності розчину.

Енергозабезпечення:

– Стабільні джерела живлення з резервним джерелом (акумулятори).

Програмне забезпечення:

– Гнучкі мови програмування: C++ (Arduino), MicroPython (Raspberry Pi Pico).

Підключення:

Блок живлення системи підключається до мережі змінного струму 220В (+15/-15%), 50 Гц (±1 Гц).

Дотримання цих вимог забезпечить створення ефективної та надійної кіберфізичної системи для контролю процесів у гідропонній теплиці, що сприятиме оптимальному росту рослин та підвищенню загальної продуктивності.

2.1.3.4 Вимоги до організаційного забезпечення

Для забезпечення ефективної роботи комп'ютерної та кіберфізичної системи в компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ» необхідно врахувати наступні організаційні аспекти:

Чіткий розподіл відповідальності: Кожен аспект функціонування системи повинен мати відповідальну особу: адміністраторів, технічних фахівців, операторів та менеджерів з безпеки.

Планування та контроль: Розробка та затвердження керівництвом плану управління системою, що включає графіки обслуговування, оновлення та процедури реагування на інциденти, є обов'язковим.

Технічна документація: Наявність повної та актуальної технічної документації з інструкціями з монтажу, налаштування та обслуговування є важливою умовою для успішної експлуатації системи.

Інструкції для користувачів: Створення зрозумілих посібників для співробітників, які працюють з системою, допоможе їм ефективно використовувати її функціонал та дотримуватися правил безпеки.

Навчання персоналу: Проведення первинного та періодичного навчання персоналу забезпечить їхню обізнаність щодо новітніх технологій та змін у роботі системи.

План аварійного відновлення: Наявність плану з процедурами резервного копіювання, відновлення системи та управління ризиками є необхідним для мінімізації наслідків можливих збоїв.

План безперервності бізнесу: Цей план визначить критичні процеси та дії для підтримки діяльності компанії у разі аварійних ситуацій.

Регулярні аудити: Проведення регулярних аудитів системи допоможе оцінити її відповідність вимогам, виявити вразливості та перевірити ефективність заходів безпеки.

Врахування цих вимог забезпечить стабільну та безперебійну роботу комп'ютерної та кіберфізичної системи, що сприятиме успішному розвитку компанії «ГРІН ФЬЮЧЕР ІНЖИРІНГ».

2.1.3.5 Вимоги до методичного забезпечення

- Візуалізація структури комплексу технічних засобів.
- Проектування топології корпоративної мережі.
- Складання таблиці адрес пристроїв.
- Формування переліку характеристик обладнання.
- Створення переліку характеристик структурованої кабельної мережі.
- Розробка плану розміщення кабельних мереж.

2.1.3.6 Вимоги до методичного забезпечення

Вимоги не надаються.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітерктури мережі підприємства

Розробка загальної архітектури мережі підприємства враховує потреби бізнесу, вимоги до безпеки та продуктивності. Вона складається з маршрутизаторів, які з'єднують різні сегменти мережі, та комутаторів, що забезпечують з'єднання робочих станцій і серверів в межах однієї підмережі. Робочі станції є кінцевими пристроями для співробітників, а сервери надають різноманітні послуги. Для зв'язку між маршрутизаторами використовуються спеціальні кабелі Serial DTE або крос-кабелі. Підключення маршрутизаторів і робочих станцій до комутаторів здійснюється прямими кабелями. Для забезпечення високої доступності та відмовостійкості мережі комутатори з'єднуються між собою крос-кабелями.

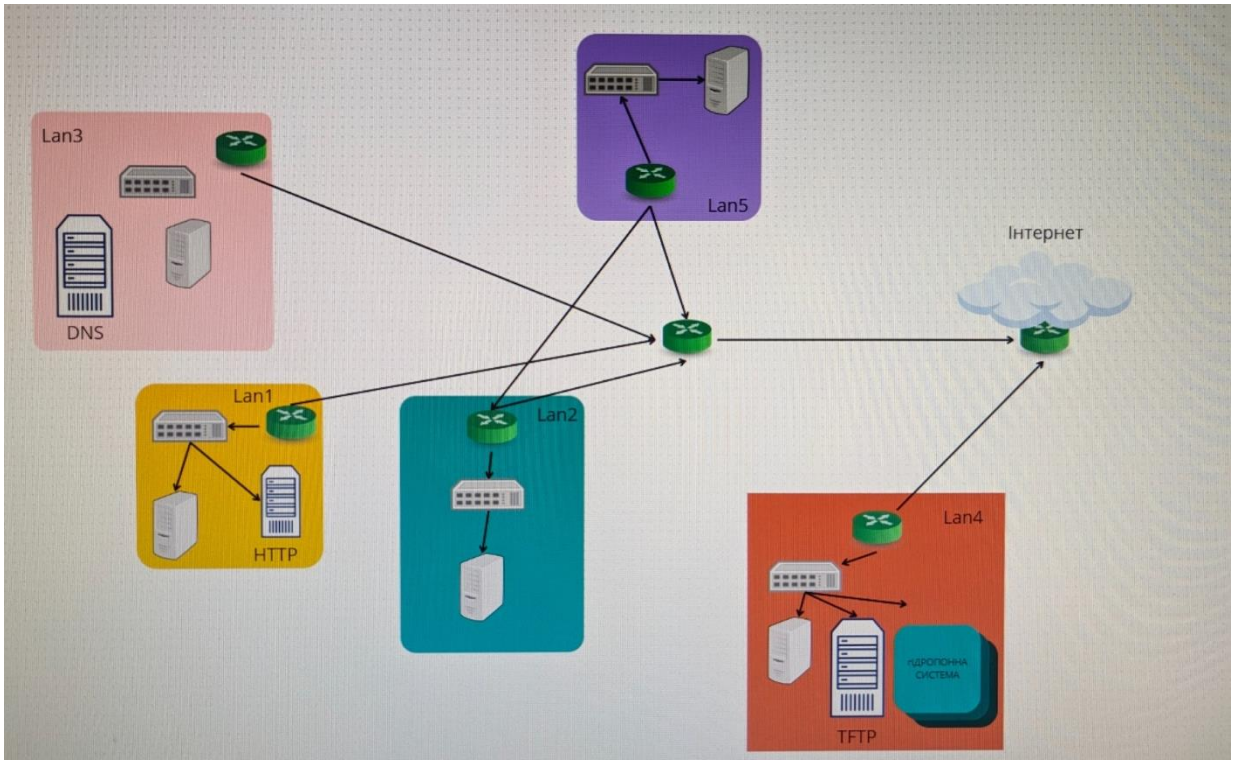

Рисунок 2.1 – Структурна схема комплексу технічних засобів системи

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

Структурна схема комплексу технічних засобів системи розроблена з метою забезпечення ефективної, надійної та безпечної роботи корпоративної мережі. Вона включає в себе наступні ключові компоненти:

Маршрутизатор Cisco 2911, високопродуктивний маршрутизатор з двома WAN портами та дев'ятьма портами для підключення комутаторів, що забезпечує швидкість обробки даних до 5 Гбіт/с. Його вибір обумовлений необхідністю забезпечення високої пропускної здатності та розширених можливостей управління мережею.

Комутатор Cisco 2960-24TT з 24 портами Fast Ethernet, що підтримує VLAN, QoS, STP та ACLs. Завдяки цьому він забезпечує не тільки швидку передачу даних, але й розширені можливості управління, безпеки та масштабованості мережі.

Маршрутизатор Ubiquiti EdgeRouter X. Він відрізняється високою продуктивністю, надійністю та широким спектром функцій, включаючи підтримку VPN, QoS та можливість гнучкого налаштування маршрутизації.

Запропонована структурна схема дозволяє створити гнучку, масштабовану та безпечну мережу, здатну задовольнити потреби сучасного підприємства. Вибір конкретних моделей обладнання обумовлений їх технічними характеристиками, функціональністю та відповідністю вимогам проекту.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	Cisco 2911.	Chorny_R1 Chorny_R2 Chorny_R3 Chorny_R4 Chorny_R5 Chorny_R0	Од.	6

2	Cisco 2960-24TT	Chorny_SW1 Chorny_SW2 Chorny_SW3 Chorny_SW4	Од.	4
3	Ubiquiti EdgeRouter X	Chorny_W	Од.	1

2.2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі LAN3 встановлений комутатор Cisco2960, що об’єднує 208 ПК працівників. Вихідний трафік з комутатора надсилається до роутера в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=148 (кадрів/с), а середня довжина повідомлення – 1150 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі DLS одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$Рр.р. = \mu * Lпов * N * 8 = 148 * 1150 * 208 * 8 = 28.3 \text{ Мбіт/с} \quad (2.1)$$

де Lпов – середня довжина повідомлення;

N – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор також передає трафік до маршрутизатора зі швидкістю 1000 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu вих = 109 / (1150 * 8) = 108\ 696 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 148 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu вих / \mu = 108\ 696/ 148 \approx 734 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 208 ПК.

Кожен з 208 ПК посилає потік заявок з інтенсивністю у 148 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 208 *148 = 30784 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{30784}{108696} = 0{,}28 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}28}{1-0{,}28} = 0{,}38 \quad (2.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696 - 30784)} = 12{,}83 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$Lчер = \frac{\rho^2}{1-\rho} = \frac{0{,}28^2}{1-0.28} = 0.109 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$Tоч = \frac{Lчер}{\lambda} = \frac{0{,}109}{254540} = 3{,}54 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології мережі

Корпоративна мережа побудована на основі комутаторів та маршрутизаторів, що забезпечують зв'язок між відділами та сегментами. Використання технології VLAN дозволяє логічно розділити мережеві ресурси відповідно до функціональних потреб, не змінюючи фізичної структури. Це підвищує безпеку та оптимізує трафік, що особливо актуально для великих корпоративних мереж.

На рисунку 3.1 представлена схема корпоративної мережі, що складається з основної та віддаленої мережі, а також мережі провайдера. З'єднання між ними здійснюється за допомогою кабелів SerialEthernet та GigabitEthernet.

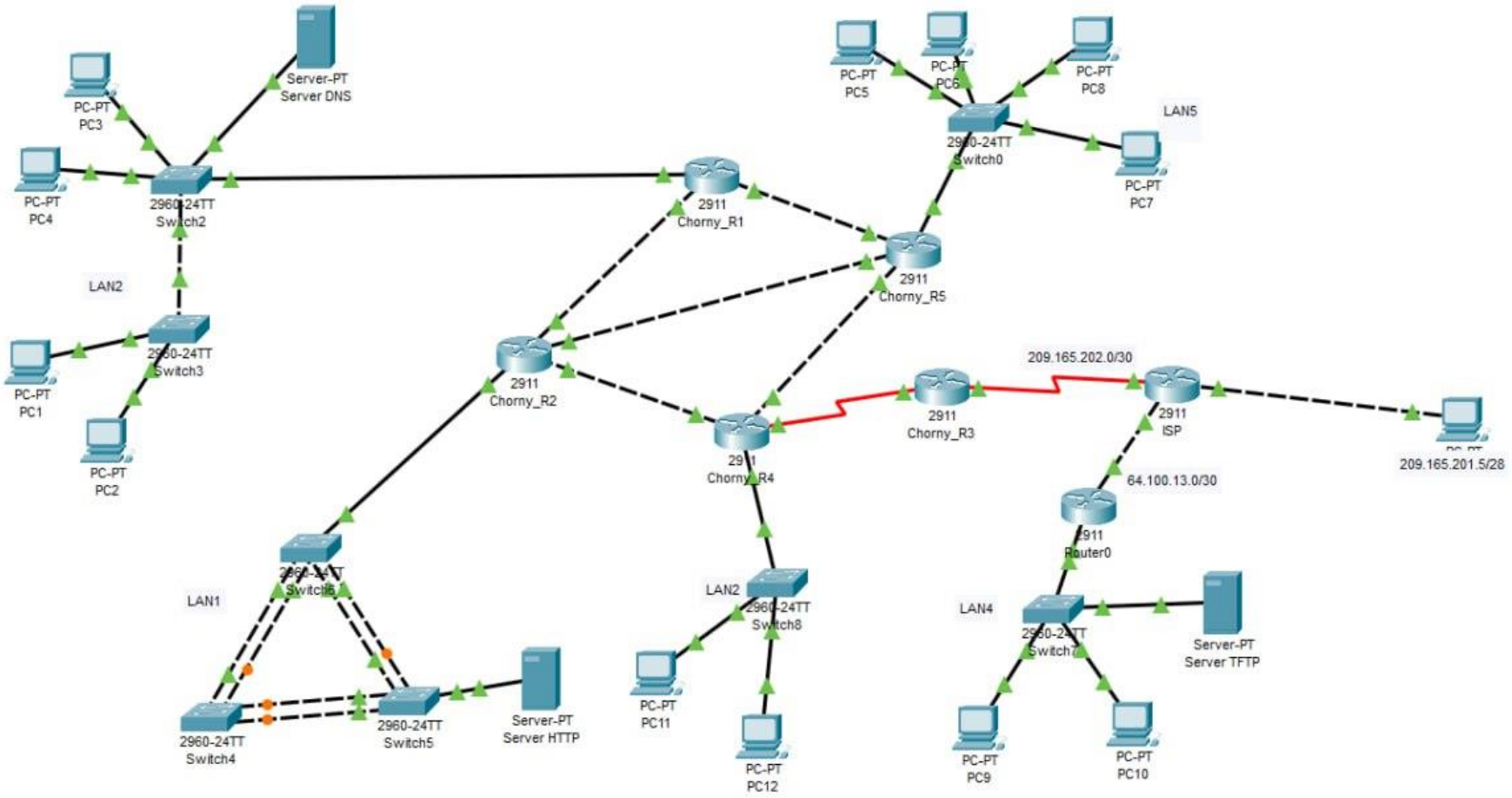

Рисунок 3.1 - Топологічна схема корпоративної мережі

3.2 Вибір та опис мережного обладнання

Для створення надійної та продуктивної мережі компанії " ГРІН ФЬЮЧЕР ІНЖИРІНГ " було обрано комутатори Cisco 2960 та маршрутизатори Cisco 2911, відомі своєю якістю та ефективністю.

Комутатори Cisco 2960 є частиною лінійки Cisco Catalyst. Вони забезпечують живлення підключених пристроїв через Ethernet (PoE), що спрощує розгортання VoIP телефонів, IP камер та іншого обладнання без додаткових кабелів живлення. Різноманітність портів, включаючи Gigabit Ethernet, забезпечує високу швидкість передачі даних, необхідну для сучасних корпоративних мереж.

Маршрутизатори Cisco 2911 належать до серії Cisco ISR (Integrated Services Routers) та призначені для роботи у складних мережах з високими вимогами. Модульна конструкція дозволяє легко додавати нові інтерфейси та сервіси. Завдяки вбудованому шифруванню та підтримці VPN, маршрутизатори гарантують безпеку передачі даних між різними офісами компанії.

Вибір такого обладнання для " ГРІН ФЬЮЧЕР ІНЖИРІНГ " обумовлений його надійністю, простотою управління та можливістю масштабування, що дозволяє компанії адаптувати мережеву інфраструктуру до зростаючих потреб бізнесу.

3.3 Розрахунок схеми адресації корпоративної мережі

Розбиття мережі на підмережі – це процес поділу великого діапазону IP-адрес на менші, незалежні частини. У таблиці 3.1 наведено приклад такого розбиття з зазначенням кількості вузлів у кожній підмережі.

Таблиця 3.1 – Блок адрес мережі та кількість вузлів в кожній підмережі

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
19	172.24.200.0/24	5	101	208	85	57

Завдання полягає в розробці п'яти підмереж, здатних підтримувати 331 користувача, з використанням методології VLSM (Variable Length Subnet Masking). VLSM надає можливість гнучкого поділу IP-адресного простору, створюючи

підмережі з різними розмірами масок, що дозволяє адаптувати мережу до потреб користувачів. Цей підхід оптимізує використання IP-адрес, підвищує ефективність ресурсів та спрощує управління мережею, забезпечуючи її масштабованість та адаптивність.

Таблиця 3.2 – Схема адресації мережі

Назва підмережі	Необхідна кіл-ть вузлів	Адреса підмережі	Маска Підмережі у Десятковому	Діапазон допустимих IP-адрес вузлів
LAN1	5	172.24.202.64	/28	72.24.202.65 - 172.24.202.70
LAN2	101	172.24.201.0	/25	172.24.201.1 - 172.24.201.126
LAN3	208	172.24.200.0	/24	172.24.200.1 - 172.24.200.254
LAN4	85	172.24.201.128	/25	172.24.201.129 - 172.24.201.254
LAN5	57	172.24.202.0	/26	172.24.202.1 - 172.24.202.62

Для організації зв'язку між маршрутизаторами виділено адресний блок 172.24.210.0/24. Застосовуючи метод VLSM (Variable Length Subnet Mask), цю мережу буде сегментовано на п'ять підмереж, кожна з яких призначена для підключення двох вузлів. Детальний план адресації каналів між маршрутизаторами наведено у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
WAN1	2	172.24.210.0	/30	172.24.210.1	172.24.210.2
WAN2	2	172.24.210.4	/30	172.24.210.5	172.24.210.6
WAN3	2	172.24.210.8	/30	172.24.210.9	172.24.210.10
WAN4	2	172.24.210.12	/30	172.24.210.13	172.24.210.14

WAN5	2	172.24.210.16	/30	172.24.210.17	172.24.210.18
WAN6	2	172.24.210.20	/30	172.24.210.21	172.24.210.22

У таблиці 3.4 наведена адресація всіх маршрутизаторів мережі.

Таблиця 3.4 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Chorny_R1	Gig0/2	172.24.210.1	255.255.255.252
	Gig0/0	172.24.210.5	255.255.255.252
	Gig0/1	VLAN	VLAN
Chorny _R2	Gig0/1	172.24.210.6	255.255.255.252
	Gig0/0	172.24.210.9	255.255.255.252
	Gig0/2	172.24.210.13	255.255.255.252
	Gig1/0	172.24.202.65	255.255.255.232
Chorny _R3	Se0/0/0	209.165.202.1	255.255.255.252
	Se0/0/1	172.24.210.17	255.255.255.252
Chorny _R4	Se0/0/0	172.24.210.10	255.255.255.252
	Gig0/0	172.24.210.18	255.255.255.252
	Gig0/2	172.24.210.21	255.255.255.252
	Gig0/1	172.24.201.1	255.255.255.128
Chorny _R5	Gig0/0	172.24.210.2	255.255.255.192
	Gig0/1	172.24.210.14	255.255.255.252
	Gig0/2	172.24.210.22	255.255.255.252
	Gig1/0	172.24.201.1	255.255.255.128
Chorny _R0	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	172.24.201.128	255.255.255.128

3.4 Вибір та налаштування способу маршрутизації

3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі Chorny _R3:

hostname Chorny_R3// призначення назви пристрою

line console 0 // вхід в конфігураційний режим лінії консолі

password cisco // призначення паролю до консолі

login // вимикання анонімного доступу

line vty 0 15 // вхід в конфігураційний режим лінії VTY

password cisco // призначення паролю до лінії VTY

login // вимикання анонімного доступу

enable secret class // встановлення зашифрованого паролю для привілейного режиму

service password-encryption // шифрування паролів

banner motd # Chorny_R3# // налаштування банера MOTD

line vty 0 15 // вхід в конфігураційний режим лінії VTY

transport input ssh // назначення використання протоколу SSH

login local // налаштування локальної аутентифікації

username 12321ck1_Chorny password admincisco // призначення імені користувача та паролю

ip domain-name Chorny_R3// налаштування імені домена

crypto key generate rsa // створення ключа шфируваня

1024 // вибір довжини ключа шифрування

int se0/0/0 // вибір DCE-інтерефейсу

clock rate 128000 // встановлення значення тактової частоти

int se0/0/1

clock rate 128000

У мережі LAN_1 застосовується технологія Etherchannel, яка дає змогу об'єднати декілька фізичних портів комутатора в один логічний канал для підвищення пропускної здатності та забезпечення резервування.

Налаштування Etherchannel на комутаторі:

interface range fa0/1-2 // вибір інтерфейсів

channel-group 1 mode active // налаштування режиму портової групи

interface port-channel 1 // вибір інтерфейсу портової групи

switchport mode trunk // налаштування портової групи в режим транку

switchport trunk allowed vlan all // встановлення всіх VLAN як дозволених для проходженя даних через транковий порт

interface range fa0/3-4

channel-group 2 mode active

interface port-channel 2

switchport mode trunk

switchport trunk allowed vlan all

3.4.2 Налаштування протоколу OSPF та DHCP для маршрутизаторів корпоративної мережі

Протокол DHCP відіграє ключову роль в оптимізації роботи мережі, автоматично призначаючи IP-адреси пристроям. Це не тільки спрощує процес налаштування нового обладнання, але й звільняє адміністраторів від рутинної роботи, дозволяючи їм зосередитися на більш важливих завданнях. Крім того, автоматизація розподілу адрес знижує ймовірність людських помилок, забезпечуючи більш стабільну та ефективну роботу мережі.

Налаштування DHCP на прикладі маршрутизатора Chorny _R5:

ip dhcp excluded-address 172.24.136.129 172.24.136.134 // виключення вказаних адрес з dhcp пулів

ip dhcp excluded-address 172.24.136.255

ip dhcp excluded-address 172.24.136.254

ip dhcp pool LAN-2 // створення та вказання адреси dhcp пулу

network 172.24.202.0 255.255.255.192 // вказання IP-адреси мережі

default-router 172.24.202.1// вказання IP-адреси шлюзу

dns-server 172.24.200.130 // вказання IP-адреси dns сервера

Для забезпечення зв'язку між користувачами з різних підмереж необхідно налаштувати обмін маршрутною інформацією. Існує два основних підходи: статичний, де маршрути задаються вручну, та динамічний, де вони оновлюються автоматично, забезпечуючи більшу гнучкість і спрощуючи управління мережею.

У нашому проекті ми будемо використовувати динамічний протокол маршрутизації OSPF, який є одним з найпоширеніших у сучасних мережах. OSPF використовує алгоритм Дейкстри (SPF) для визначення найкоротших шляхів передачі даних, що значно покращує швидкість роботи мережі. Серед інших переваг OSPF

варто відзначити його масштабованість, високий рівень безпеки, підтримку VLSM (масок змінної довжини) та сумісність з обладнанням різних виробників.

Застосування динамічної маршрутизації за допомогою OSPF дозволить нам ефективно керувати мережевим трафіком, забезпечуючи стабільність і високу продуктивність нашої мережі.

Налаштування протоколу OSPF на прикладі маршрутизатора Chorny _R3:

router ospf 1 // увімкнення протоколу

network 172.24.210.12 0.0.0.3 area 0 // анонсування всіх необхідних для маршрутизації мереж

network 209.165.202.0 0.0.0.3 area 0

passive-interface default // відключення поширення оновлень за замовчуванням на всіх портах

no passive-interface Serial0/0/0 // увімкнення поширення оновлень на портах, через які будуть передаватись дані щодо підключених мереж

no passive-interface Serial0/0/1

На межовому маршрутизаторі встановлюємо шлях за замовчуванням, який веде до маршрутизатора провайдера інтернет-послуг, і забезпечуємо його поширення.

ip route 0.0.0.0 0.0.0.0 209.165.202.2 // налаштовуємо маршрут за замовчуванням

router ospf 1 // увімкнення протоколу

redistribute static subnets // увімкнення розповсюдження статичних маршрутів через протокол OSPF

Встановлюємо постійний маршрут до мережі інтернет-провайдера:

ip route 209.165.201.0 255.255.255.240 209.165.202.2

3.4.3 Налаштування роботи Інтернет

Для забезпечення доступу до Інтернету система використовує технологію NAT (Network Address Translation), яка дозволяє трансформувати внутрішні IP-адреси, що використовуються в локальній мережі, у публічні, які використовуються в Інтернеті.

Завдяки цьому, множина пристроїв може одночасно виходити в Інтернет, використовуючи обмежену кількість публічних IP-адрес.

Для здійснення NAT-трансляції необхідно створити набір публічних IP-адрес, який буде використовуватися для заміни внутрішніх адрес при зверненні до Інтернету. Наприклад, можна виділити діапазон від 209.165.202.5 до 209.165.202.30. Цей набір адрес буде застосовуватися для перетворення внутрішніх адрес у публічні та навпаки, забезпечуючи коректну маршрутизацію трафіку між локальною мережею та Інтернетом.

Розглянемо конфігурацію NAT на основі прикладу пограничного маршрутизатора Chorny _R3:

```
ip access-list extended NAT19
deny ip 172.24.201.0 0.0.0.127 172.24.201.128 0.0.0.127
deny ip 172.24.200.0 0.0.0.255 172.24.201.128 0.0.0.127
deny ip 172.24.202.64 0.0.0.15 172.24.201.128 0.0.0.127
deny ip 172.24.202.0 0.0.0.63 172.24.201.128 0.0.0.127
deny ip 172.24.210.0 0.0.0.255 172.24.201.128 0.0.0.127
permit ip 172.24.201.0 0.0.0.127 any
permit ip 172.24.200.0 0.0.0.255 any
permit ip 172.24.202.64 0.0.0.15  any
permit ip 172.24.202.0 0.0.0.63  any
permit ip 172.24.210.0 0.0.255.255 any
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip nat inside source static 172.24.200.130 209.165.200.3
interface Serial0/0/0
ip nat outside
interface Serial0/0/1
```

3.5 Налаштування мереж VLAN, маршрутизації між VLAN

VLAN – це потужний інструмент мережевої віртуалізації, який дозволяє розділити одну фізичну мережу на декілька незалежних логічних сегментів. Це забезпечує гнучкість у керуванні мережевим трафіком, дозволяючи налаштовувати окремі правила та політики безпеки для кожної віртуальної мережі, що відповідає потребам конкретних груп користувачів чи пристроїв. Завдяки VLAN, відпадає необхідність фізичного розмежування мережі за допомогою додаткових кабелів та комутаторів, що значно спрощує її адміністрування та знижує витрати на обладнання.

Крім того, VLAN підвищує безпеку мережі, створюючи ізольовані середовища для різних груп користувачів, що ускладнює несанкціонований доступ до даних та мінімізує ризики внутрішніх атак. Таким чином, VLAN є невід'ємною частиною сучасних мережевих інфраструктур, забезпечуючи їх ефективність, безпеку та керованість.

Таблиця 3.5 – Адресація мереж VLAN

Назва	Мережева адреса	Маска	Діапазон використання
VLAN10	172.24.200.0	/26	172.24.200.1 - 172.24.200.62
VLAN20	172.24.200.64	/26	172.24.200.65 - 172.24.200.126
VLAN30	172.24.200.128	/26	172.24.200.129 - 172.24.200.190
VLAN99	172.24.200.192	/28	172.24.200.193 - 172.24.200.222

Налаштування VLAN на прикладі комутатора з мережі LAN3:

int range fa0/5-10 // вибір портів

switchport mode access // налаштування портів

switchport access vlan 10 // присвоювання портам влану

int range fa0/11-16

switchport mode access

switchport access vlan 20

int range fa0/17-24

switchport mode access

switchport access vlan 30

int range fa0/1-4

switchport mode trunk // налаштування портів в режим транку

switchport trunk native vlan 100 // налаштування власної мережі на транковому порті

switchport trunk allowed vlan 42,22,32,99-100 //налаштування списку дозволених VLAN на транковому порті

int vlan 99 // вибір VLAN

ip address 172.24.200.192 255.255.255.240 // призначення IP-адреси

ip default-gateway 172.24.200.193 // вказання IP-адреси шлюзу за замовчуванням

Налаштовуємо підінтерфейси на маршрутизаторі Myxin_R1, що будуть виступати в ролі шлюзу для вказаних VLAN:

int g0/1.10 // вибір підінтерфейсу

encapsulation dot1Q 10 // встановлення мітки для вибраного порту

ip address 172.24.200.65 255.255.255.192 // вказання IP-адреси підінтерфейсу

int g0/1.20

encapsulation dot1Q 20

ip address 172.24.200.1 255.255.255.192

int g0/1.30

encapsulation dot1Q 30

ip address 172.24.200.129 255.255.255.192

int g0/1.99

encapsulation dot1Q 99

ip address 172.24.200.193 255.255.255.240

Для автоматичного призначення IP-адрес вузлам в різних VLAN буде використовуватись протокол DHCP. Налаштування DHCP на маршрутизаторі Myxin_R1, який буде виступати в ролі DHCP-сервера:

ip dhcp excluded-address 172.24.137.1 172.24.137.5

ip dhcp excluded-address 172.24.137.65 172.24.137.70

ip dhcp excluded-address 172.24.200.129 172.24.200.131

ip dhcp pool LAN-VLAN10

network 172.24.200.0 255.255.255.192

default-router 172.24.200.1

dns-server 172.24.200.130

ip dhcp pool LAN-VLAN20

network 172.24.200.64 255.255.255.192

default-router 172.24.200.65

dns-server 172.24.200.130

ip dhcp pool LAN-VLAN30

network 172.24.200.128 255.255.255.192

default-router 172.24.200.129

dns-server 172.24.200.130

3.6 Перевірка комп’ютерної Системи підприємства

Проведено перевірку базових налаштувань обладнання за допомогою команди show running-config у привілейованому режимі аналізується ряд параметрів, таких як ім'я пристрою, налаштування паролів для доступу до консолі та ліній vty, їх конфігурація для використання протоколу ssh, пароль для доступу до привілейованого режиму, налаштування банера MOTD і ім'я домену.

```
hostname Chorny_R2
```

Рисунок 3.1 – Назва пристрою

```
line con 0
 password 7 0822455D0A16
 login
```

Рисунок 3.2 – Пароль до консольного режиму

```
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
```

Рисунок 3.3 – Пароль до ліній vty та використання на них протоколу ssh

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

Рисунок 3.4 – Пароль до привілейованого режиму

```
!
banner motd ^CChorny_R2^C
!
```

Рисунок 3.5 – Банер MOTD

```
!
hostname Chorny_R2
!
```

Рисунок 3.6 – Ім’я домена

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

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

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

1      Po1(SU)           LACP      Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP      Fa0/3(P) Fa0/4(P)
```

Рисунок 3.7 – Технологія EtherChannel

Як бачимо з рис. 3.12, зв’язок між різними підмережами на прикладі підмереж LAN_4 та LAN_5 є успішним

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC9	ICMP		0.000	N	0	(edit)	(delete)
	Successful	TFTP	PC9	ICMP		0.000	N	1	(edit)	(delete)

Рисунок 3.8 – Зв’язок між LAN_4 та LAN_5

```
     209.165.201.0/28 is subnetted, 1 subnets
S       209.165.201.0 [1/0] via 209.165.202.2
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.9 – Налаштуваний маршрут за замовчуванням на маршрутизаторі

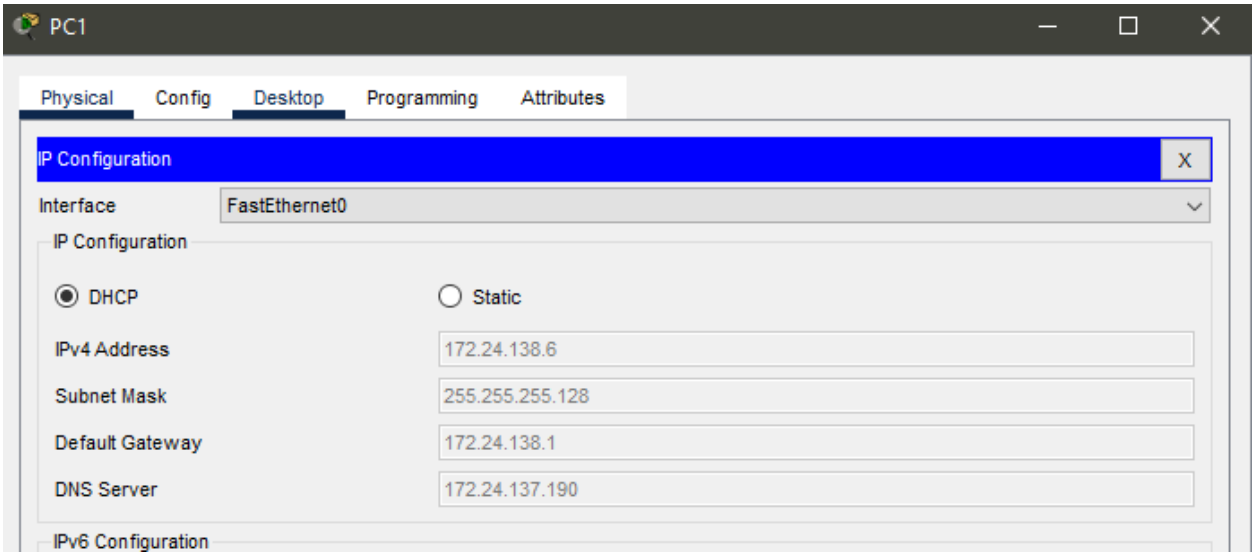

Рисунок 3.10 – IP-адреса PC1

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
20   VLAN0020                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16
30   VLAN0030                          active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Рисунок 3.11 – Імена та порти VLAN

```
Switch#show interfaces tr
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30
Fa0/2       1,10,20,30
Fa0/3       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30
Fa0/2       1,10,20,30
Fa0/3       1,10,20,30
```

Рисунок 3.12 – Транкові порти

Як бачимо, зв’язок між PC14 та PC13, які знаходять в VLAN10 та VLAN20 відповідно, є успішним.

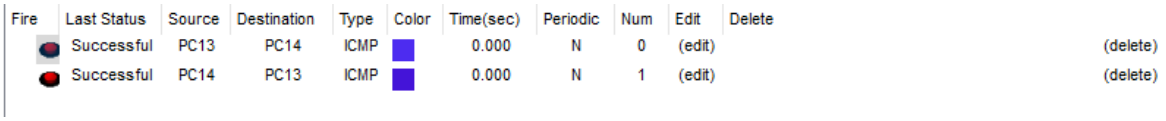

Рисунок 3.13 – Зв’язок між VLAN10 та VLAN20

Тестуємо доступність веб-ресурсу, що містить інформацію про тему та завдання кваліфікаційної роботи студента, використовуючи PC11 як приклад.

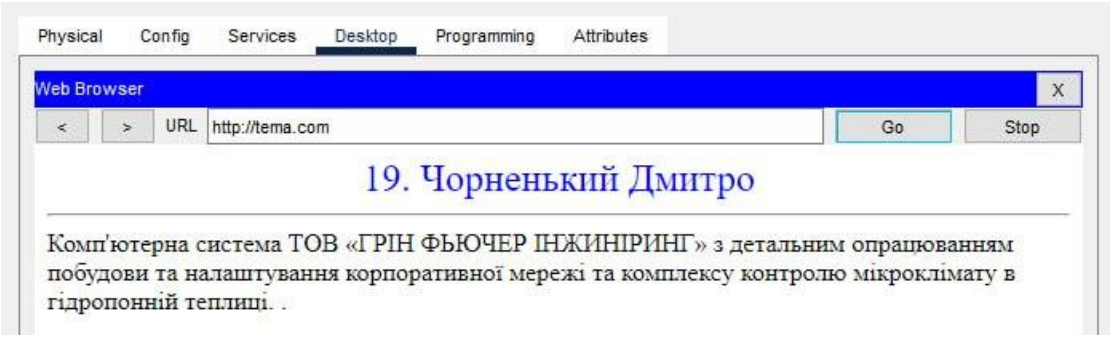

Рисунок 3.14 – Відкритий веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Проектування 3D-моделі компонента

4.1.1 Вибір програмного забезпечення для 3D-моделювання.

Для створення 3D-моделей компонентів системи контролю процесів живлення в гідропонній теплиці було обрано програмне забезпечення FreeCAD. Цей вибір обумовлений кількома факторами:

– Безкоштовність та відкритий код: FreeCAD є вільно розповсюджуваним програмним забезпеченням з відкритим вихідним кодом, що дозволяє використовувати його безкоштовно та вносити зміни до коду за потреби. Це особливо важливо для проектів з обмеженим бюджетом.

– Параметричне моделювання: FreeCAD підтримує параметричне моделювання, що дозволяє легко змінювати розміри та форму моделей, редагуючи параметри. Це значно спрощує процес внесення змін та оптимізації конструкції.

– Модульність та розширюваність: Функціональність FreeCAD може бути розширена за допомогою додаткових модулів, що дозволяє адаптувати його до специфічних потреб проекту.

– Кросплатформеність: FreeCAD працює на різних операційних системах (Windows, macOS, Linux), що забезпечує гнучкість у виборі робочого середовища.

Рисунок 4.1 – Логотип програмного забезпечення для моделювання FreeCAD.

Переваги FreeCAD в контексті даного проекту:

– Простота використання: Інтерфейс FreeCAD інтуїтивно зрозумілий та легкий у вивченні, що дозволяє швидко освоїти основні інструменти моделювання.

– Достатній функціонал: FreeCAD має всі необхідні інструменти для створення моделей компонентів системи контролю, включаючи геометричне моделювання, складання та створення технічних креслень.

– Підтримка експорту в різні формати: FreeCAD дозволяє експортувати моделі у формати, сумісні з більшістю програм для слайсингу та 3D-друку (STL, OBJ).

В цілому, FreeCAD є оптимальним вибором для даного проекту завдяки своїй безкоштовності, параметричному моделюванню та достатньому функціоналу для створення моделей компонентів системи контролю процесів живлення в гідропонній теплиці.

4.1.2 Опис функціонального призначення компонента та його ролі в системі.

У рамках розробки комплексної системи контролю процесів живлення в гідропонній теплиці важливим етапом є проектування та виготовлення її фізичних компонентів. Для цього було використано 3D-моделювання та друк, що дозволяє швидко та ефективно створювати прототипи та деталі необхідної конфігурації.

Опис 3D-моделей:

Маленька тара для реагентів:

– Функціональне призначення: Зберігання та дозування поживних речовин (реагентів), необхідних для росту рослин у гідропонній системі.

– Роль у системі: Забезпечення точного дозування реагентів у живильний розчин, що подається до коріння рослин.

– Особливості конструкції: Компактна та герметична ємність з розмірами 100мм * 100мм * 200мм з отворами для підключення до системи дозування та контролю рівня рідини.

Всього буде виготовлено дві такі ємності. Кожна ємність обладнана захисною кришкою, отвором для під'єднання до гідропонної системи та датчиком рівня рідини (water sensor).

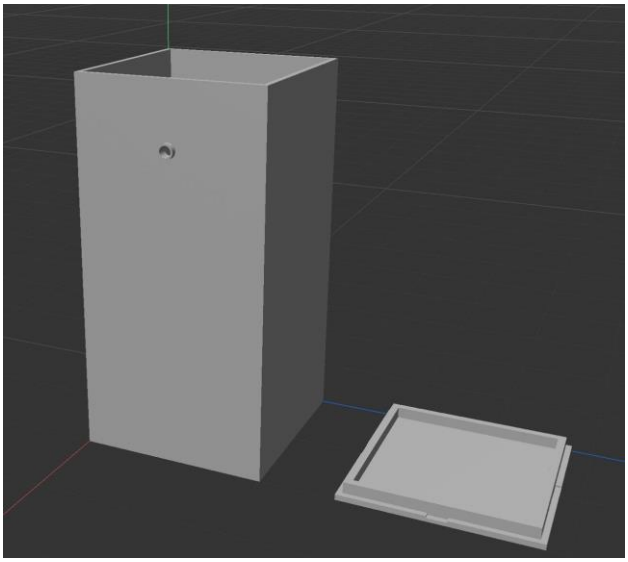

Рисунок 4.2 – 3D модель малої тари для зберігання реагентів

Датчик рівня рідини дозволить контролювати наявність реагентів у ємності та своєчасно їх поповнювати. Захисна кришка запобігатиме потраплянню сторонніх речовин та випаровуванню реагентів.

Велика тара для води:

– Функціональне призначення: Зберігання запасу води, що використовується для приготування живильного розчину.

– Роль у системі: Забезпечення безперебійної подачі води до системи поливу та підтримки стабільного рівня вологості в теплиці.

– Особливості конструкції: Велика ємність з міцними стінками розміром 200 мм * 100 мм * 200 мм, отворами для підключення до системи поливу та контролю рівня води.

Буде виготовлено одну ємкість. Вона буде оснащена захисною кришкою, яка запобігає потраплянню забруднень у воду та випаровуванню вологи. Отвір для під'єднання до гідропонної системи забезпечує зручність наповнення та спорожнення

тари. Датчик рівня води дозволяє автоматично контролювати кількість води в тарі та своєчасно поповнювати її запаси.

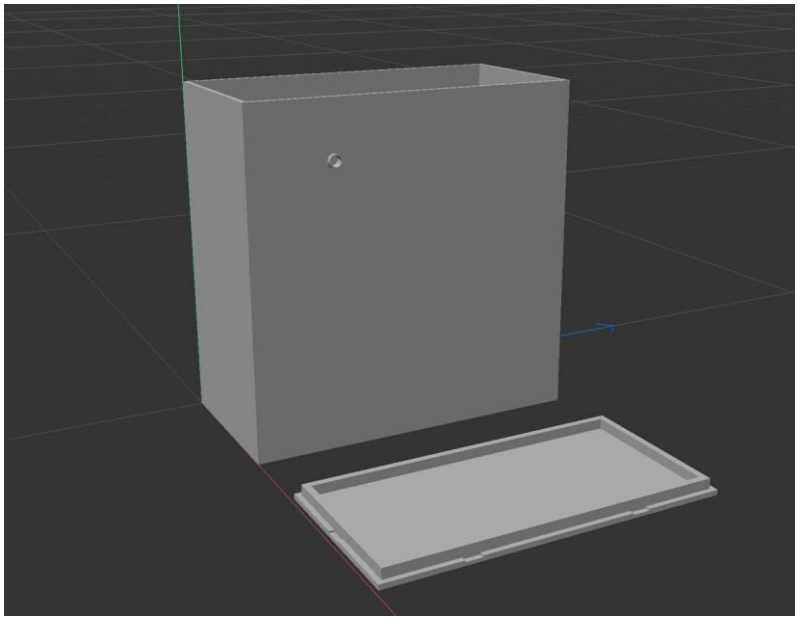

Рисунок 4.3 – 3D модель великої тари для зберігання питної води.

Зона зберігання тар для води та реагентів:

– Функціональне призначення: Організація зручного та безпечного зберігання тар з водою та реагентами.

– Роль у системі: Забезпечення порядку в теплиці та запобігання випадковому розливу хімічних речовин.

– Особливості конструкції: Полиці або стелажі з урахуванням розмірів тар та вимог безпеки.

Буде виготовлено одну стійку для зберігання .

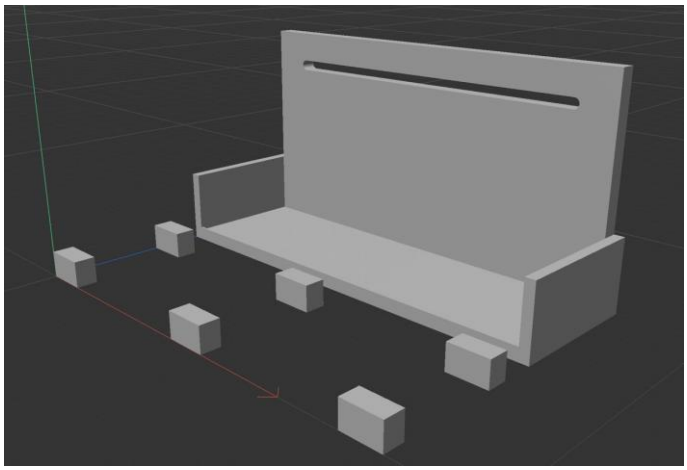

Рисунок 4.4 – 3D модель для зберігання тар з рідинами.

Зона поливу та догляду за рослинами:

– Функціональне призначення: Простір для розміщення рослин та проведення робіт з їх догляду (обрізка, підв'язка, збір врожаю).

– Роль у системі: Забезпечення оптимальних умов для росту та розвитку рослин.

– Особливості конструкції: Розміщення рослин на гідропонних установках, забезпечення доступу до кожної рослини для догляду.

Буде побудовано модель зони поливу рослин у розмірі 350мм*270мм*100мм. Вона буде оснащена трьома отворами для подачі рідин (живильного розчину та води) з тар, розташованих у зоні зберігання. Буде вмонтовано EC для точного дозування та контролю подачі рідин та pH датчиками для моніторингу кислотності живильного розчину та автоматичного коригування його складу.

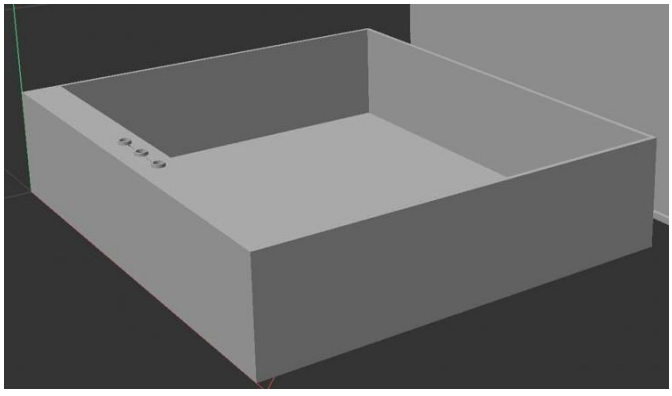

Рисунок 4.5 – 3D модель зони поливу

Ця єдина платформа поєднує в собі функції поливу та догляду за рослинами, що дозволяє оптимізувати простір у теплиці та спростити процес обслуговування рослин.

Зона освітлення:

– Функціональне призначення: Розміщення джерел штучного освітлення для забезпечення рослин необхідним світловим режимом та датчиків температури та освітлення.

– Роль у системі: Створення оптимальних умов освітлення для фотосинтезу та росту рослин, особливо в умовах недостатнього природного світла.

– Особливості конструкції:Модель являє собою єдиний корпус розміром 320 мм * 220 мм * 200 мм. Розміщення світлодіодних фіто-світильників на оптимальній висоті та з урахуванням потреб різних видів рослин.

Побудовано модель зони освітлення з врахуванням усіх вимог, щодо розмірів рослин.

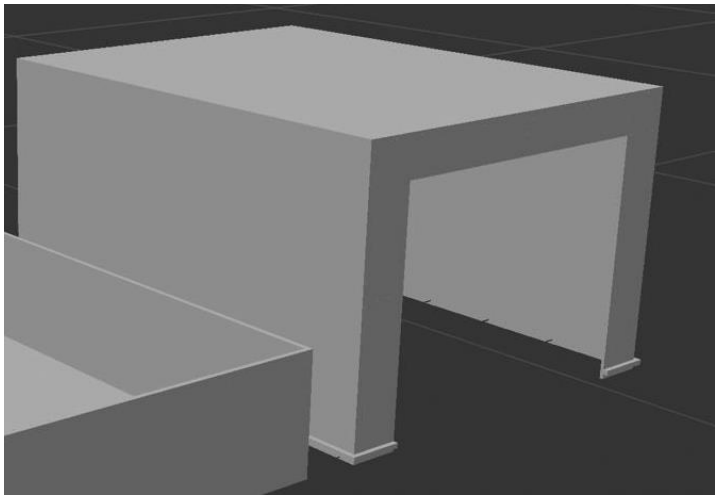

Рисунок 4.6 – 3D модель зони освітлення.

Зона керування та електронних компонентів:

– Функціональне призначення: Розміщення центрального блоку керування системою, датчиків, контролерів та інших електронних компонентів.

– Роль у системі: Забезпечення збору даних з датчиків, управління всіма процесами в теплиці, обробка та аналіз інформації.

– Особливості конструкції: Захищений корпус для електроніки, зручний доступ до елементів керування та підключення датчиків.

Буде виготовлено одну модель зони керування та електронних компонентів для збереження та встановлення таких компонентів:

Центральний блок керування: Мікроконтролер або комп'ютерна система, що відповідає за збір даних з датчиків, обробку інформації та видачу команд на виконавчі пристрої (насоси, клапани, освітлення тощо).

Блок живлення: Забезпечує електроживлення всіх компонентів системи.

Інтерфейс користувача: Дисплей та кнопки керування для налаштування параметрів системи та моніторингу її стану.

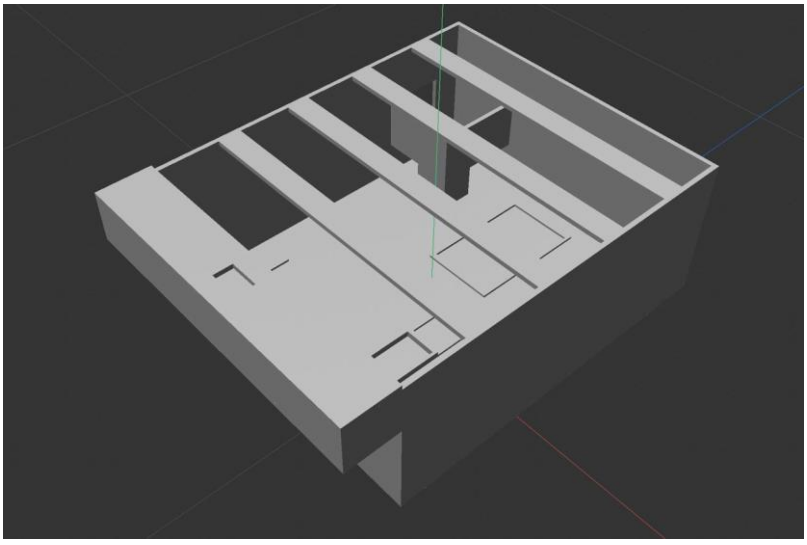

Рисунок 4.7 – 3D модель зони керування та електронних компонентів

4.2 Підготовка моделі до друку

4.2.1 Вибір програмного забезпечення для слайсингу

Слайсер – це спеціалізоване програмне забезпечення, яке відіграє ключову роль у процесі 3D-друку. Його основне завдання полягає у перетворенні тривимірної моделі об'єкта у набір інструкцій для 3D-принтера, які визначають, як саме принтер

повинен рухати екструдер та наносити матеріал шар за шаром, щоб створити фізичну копію моделі.

Основні функції слайсера:

Розбиття моделі на шари: Слайсер розрізає 3D-модель на тонкі горизонтальні шари, які потім послідовно друкуються принтером.

Генерація опорних структур: Для складних моделей, що мають нависаючі елементи, слайсер може створювати тимчасові опорні структури, які підтримують ці елементи під час друку.

Розрахунок траєкторії руху екструдера: Слайсер визначає оптимальний шлях руху екструдера для кожного шару, враховуючи швидкість друку, температуру та інші параметри.

Налаштування параметрів друку: Слайсер дозволяє налаштувати різні параметри друку, такі як висота шару, швидкість друку, температура екструдера та платформи, тип заливки тощо.

Генерація G-коду: На основі налаштувань та розрахунків слайсер створює G-код – набір інструкцій, зрозумілих для 3D-принтера, які визначають всі аспекти процесу друку.

Існує безліч різних слайсерів, як безкоштовних, так і комерційних. Деякі з найпопулярніших:

Cura - безкоштовний та зручний слайсер з великою кількістю налаштувань та підтримкою більшості 3D-принтерів.

PrusaSlicer - безкоштовний слайсер від компанії Prusa Research, оптимізований для роботи з їх принтерами, але також сумісний з іншими моделями.

У ході розробки проекту було використано Orca Slicer. Orca Slicer – це відносно новий, але швидко набираючий популярність слайсер для 3D-друку, який пропонує потужні можливості та гнучкість налаштувань. Він є повністю безкоштовним та має відкритий вихідний код, що робить його привабливим вибором для широкого кола користувачів.

Основні переваги Orca Slicer:

– Orca Slicer має інтуїтивно зрозумілий та зручний інтерфейс, що полегшує процес налаштування параметрів друку.

– Програма підтримує різноманітні функції, такі як автоматична генерація опор, адаптивне налаштування шарів, розширені налаштування заливки та багато іншого.

– Завдяки продуманим алгоритмам Orca Slicer дозволяє досягти високої якості друку навіть на бюджетних 3D-принтерах.

– Orca Slicer сумісний з більшістю популярних моделей 3D-принтерів, що робить його універсальним інструментом.

– Проект Orca Slicer активно розвивається, регулярно виходять нові версії з поліпшеннями та новими функціями. Також існує велика та активна спільнота користувачів, які готові допомогти та поділитися досвідом.

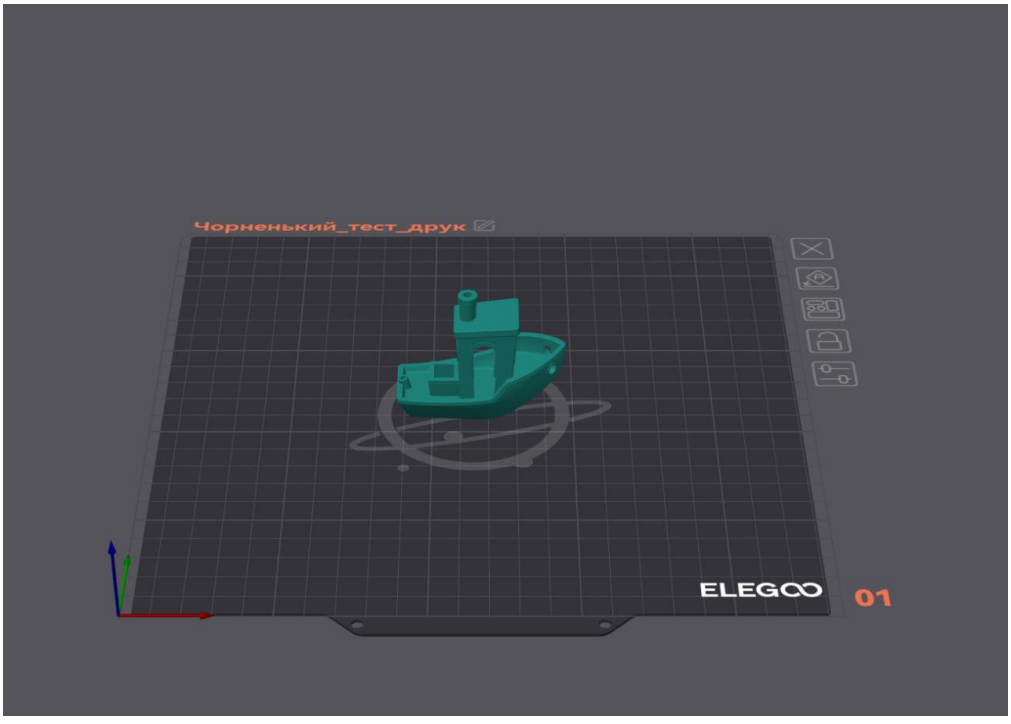

Рисунок 4.8 – Віртуальне поле для розміщення та налаштування друку 3D моделей

4.3 Інтеграція надрукованих 3D моделей у проект

Після друку усіх необхідних 3D моделей та їх пост-обробки необхідно з'єднати все разом у єдину конструкцію. У місцях стиків, де це було необхідно, використовувалася 3D-ручка для забезпечення надійного та герметичного з'єднання деталей.

Перед остаточною збіркою всі електронні компоненти, включаючи центральний блок керування, блок живлення, контролери та датчики, були розміщені та закріплені всередині корпусу зони керування. Це забезпечило захист електроніки від зовнішніх впливів та полегшило подальше підключення до системи.

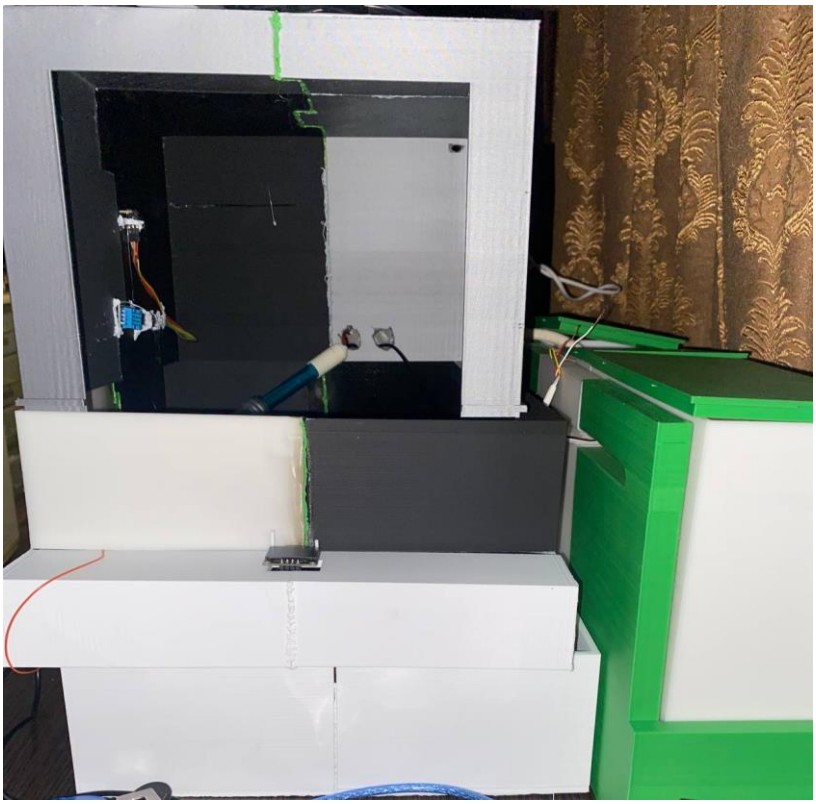

Рисунок 4.9 – Проект у процесі збірки

ВИСНОВКИ

В даній роботі було проаналізовано компанію «Грін фьючер інжирінг» та розглянуто побудову та розбиття корпоративної мережі. Також розглянуто вимоги до неї та вимоги та специфікації для системи комплексу контролю процесів живлення в гідропонній теплиці .

Був проведений ретельний огляд об’єкту розробки та прописані вимоги до комп’ютерної системи та системи гідропонної теплиці. Згідно вимог було підібрано необхідне обкладення.

Робота передбачає впровадження інноваційних рішень для автоматизації та оптимізації управління виробничими процесами.

У процесі розгляду були враховані потреби компанії у масштабуванні та розвитку системи у майбутньому, що дозволить ефективно адаптуватися до швидких змін у технологічному середовищі. Застосування передових технологій та врахування найкращих практик в галузі інформаційної безпеки гарантує стійкість та надійність системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023. – 62 с.

2. Сайт компанії «Грін фьючер інжирінг» – Education [Електронний ресурс] – Режим доступу до ресурсу: https://greenfuture.com.ua/

3. Мережа cisco – [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/products/networking/access-networking/index.html

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

5. SoftFever OrcaSlicer – [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/SoftFever/OrcaSlicer

6. FreeCAD wiki – [Електронний ресурс] – Режим доступу до ресурсу: https://wiki.freecad.org/Main_Page