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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Гречена Олексія Сергійовича
(ПІБ)
академічної групи 123-20ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему Інтелектуальна комп'ютерна система контролю виробничих процесів в Житомирській кондитерській фабриці "ЖЛ" на основі CoAP протоколу.
(назва за наказом ректора)

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

Дніпро
2023

ЗАТВЕРДЖЕНО:
Завідувач кафедри
Інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"__"_____ *2023 року*

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студенту Гречен О.С. академічної групи 123-20ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему: Інтелектуальна комп'ютерна система контролю виробничих процесів в Житомирській кондитерській фабриці "ЖЛ" на основі CoAP протоколу.
затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023р. № 350-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	9.06.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	16.062023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	23.06.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	30.06.2023

Завдання видано_____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 03.05.2023 р.

Дата подання до екзаменаційної комісії 13.07.2023 р.

Прийнято до виконання_____ Гречен О.С
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 100 с., 47 рис., табл., 14 джерел.

Об’єкт розробки: інтелектуальна комп’ютерна система контролю виробничих процесів в кондитерській фабриці “Житомирські Ласощі” з використанням CoAP протокола та з детальним опрацюванням побудови та налаштування корпоративної мережі.

Мета: розробити інтелектуальну комп’ютерну систему контролю виробничих процесів в кондитерській фабриці “Житомирські Ласощі” та основі CoAP протоколу.

Розроблена інтелектуальна комп’ютерна система спрямована на для ефективного та швидкого реагування на технічні несправності в робочий зоні виробничих процесів. Датчики контролюють стан робочих приміщень, відеокамери слідкують за правильністю виконання процесів та станом приміщення. Також інтелектуальна комп’ютерна система забезпечує виконання функцій з об’єднання підрозділів у мережу, збір обробку та накопиченню інформації на серверах.

Передача даних в розробленій інтелектуальній системи завдяки CoAP протоколу та сучасному обладнанню. Інтелектуальна комп’ютерна система виконана для майбутнього масштабування та розширення.

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

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

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

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

КС – комп’ютерна система

КМ – корпоративна мережа

ІКС – інтелектуальна комп’ютерна система

ПК – персональний комп’ютер

VLSM – Variable Length Subnet Masking

ISAKMP – Internet Security Association and Key Management Protocol

AAA – Authentication, Authorization, and Accounting

NAT – Network Address Translation

IoT – Internet of Things

CoAP – Constrained Application Protocol

VLAN – Virtual Local Area Network

DTLS – Datagram Transport Layer Security

ВСТУП

Кондитерська фабрика “Житомирські ласощі” - це відоме в Україні підприємство, яке спеціалізується на виробництві та продажі кондитерських виробів.

Бренд “Житомирські ласощі“ добре відомий клієнтам за своєю високою якістю продукту та надійною репутацією на ринку. Фабрика забезпечує високу якість своїх виробів завдяки використанню тільки натуральних інгредієнтів, виробництву продукції на сучасних обладнаннях та наявності високої кваліфікації персоналу.

Актуальність теми полягає в тому, що кондитерські фабрики мають високу конкурентну боротьбу на ринку. У зв'язку з цим, вони все більше зацікавлені у розвитку та впровадженні новітніх технологій, що дозволить підвищити якість та продуктивність виробів, зменшити ризики та витрати з виробництва та підтримувати високий рівень конкурентоспроможності на ринку.

Розробка інтелектуальної комп’ютерної системи контролю виробничих процесів на кондитерській фабриці “Житомирські ласощі” відповідає сучасним потребам та вимогам виробництва та може стати кроком до досягнення високих показників продуктивності та якості виробів. Використання спеціалізованого протоколу CoAP дозволить уникнути багатьох проблем, які зустрічаються в звичайних мережах Інтернету речей, тому система може стати важливим інструментом у розвитку не тільки кондитерської галузі, але й в інших галузях виробництва.

Отже основною метою цієї кваліфікаційної роботи є забезпечення ефективного контролю та управління виробничими процесами на фабриці, що дає змогу підвищити їх продуктивність та якість виробів, а також зменшити ризики виробничих невдач.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАДАЧІ

1.1 Стисла характеристика галузі та умов застосування

Виробництво кондитерських виробів на сьогоднішній день є досить складним та вимагає високої точності і керованості в процесі виробництва. Для забезпечення якісної і безперебійної роботи в цій галузі використовуються інноваційні рішення, такі як інтелектуальні комп’ютерні системи контролю виробничих процесів.

Інтелектуальна комп’ютерна система контролю виробничих процесів в кондитерській фабриці “Житомирські Ласощі” на основі CoAP протоколу є сучасним інструментом автоматизації виробничих процесів, що дозволяє забезпечити ефективне керування всіма етапами виробництва кондитерської продукції. Система дозволяє відстежувати рух сировини та готової продукції на всіх етапах виробництва, а також контролювати параметри виробничих процесів.

Дана система базується на протоколі CoAP, що забезпечує швидку і безперервну передачу даних між різними пристроями. Для встановлення зв'язку система використовує мережу Інтернету речей (IoT), що дозволяє забезпечити максимальну доступність і управління виробничими процесами з будь-якої точки світу.

Застосування інтелектуальної комп’ютерної системи контролю виробничих процесів в кондитерській фабриці “Житомирські Ласощі” дозволяє значно підвищити продуктивність та якість виробництва, скоротити час на виробництво та знизити витрати на управління. Ця система є надійним та ефективним інструментом для контролю виробничих процесів та підвищення конкурентоспроможності на ринку.

1.2 Характеристика і структура об’єкта впровадження

Кондитерська фабрика “Житомирські ласощ” на сьогоднішній день є однією з найбільших українських компаній у своїй галузі. Її штат налічує

близько тисячі співробітників, загальна виробнича потужність кондитерської фабрики складає понад 80 тисяч тонн продукції на рік. Крім того, фабрика продовжує розвиватися, нарощуючи свої виробничі потужності.

З метою забезпечення якісного та різноманітного асортименту продукції, на фабриці діє 7 цехів з 7 лініями. Виробництво кондитерської фабрики включає в себе цукерки, печиво, шоколад, вафлі та без цукрову продукцію. Більшість процесів виробництва фабрика вже автоматизувала, однак для підвищення ефективності та контролю за продуктивністю виробничих процесів можна покращити завдяки інтелектуальної комп'ютерної системи контролю виробничих процесів на основі CoAP протоколу.

Щоб розробити проек мережі для кондитерської фабрики "Житомирські Ласощі", необхідно проаналізувати організаційну структуру, щоб зрозуміти які підрозділи, будуть поєднані мережею.

Організаційна структура підприємства, зокрема кондитерської фабрики "Житомирські Ласощі", передбачає наявність спеціалізованих відділів при кожному секторі діяльності компанії, які відповідають за виконання відповідних функцій.

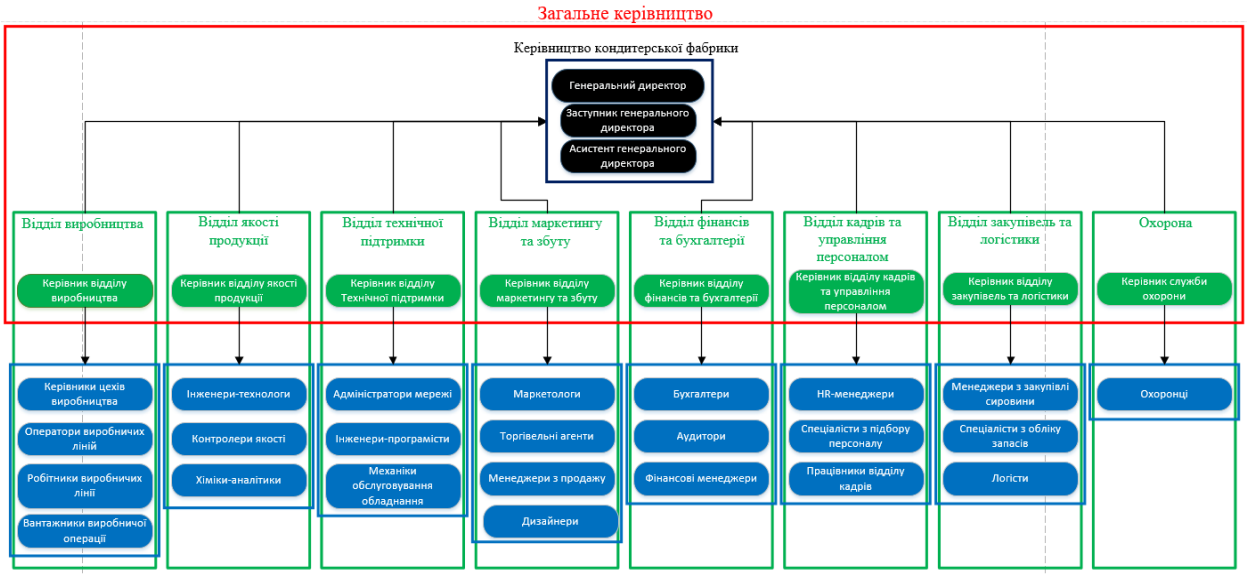

Рисунок 1.1 – Організаційна структура кондитерської фабрики "Житомирські Ласощі"

Генеральному директору підпорядковуються усі відділи та їх керівники, у генерального директора є заступник та власний асистент що допомагає з комунікацією директора з керівниками відділів та іншими працівниками.

Керівник відділу виробництва за працю:

– керівників цехів виробництва;

– операторів виробничих ліній;

– робітники виробничих ліній;

– вантажники виробничої операції.

Керівник відділу якості продукції відповідає за працю:

– інженерів-технологів;

– контролерів якості;

– хіміків-аналітиків.

Керівник відділу технічної підтримки відповідає за працю:

– адміністраторів мережі;

– інженерів-програмістів;

– механіків обслуговування обладнання.

Керівник відділу маркетингу та збуту відповідає за працю:

– маркетологів;

– торгівельних агентів;

– менеджерів з продажу;

– мизайнерів.

Керівник відділу фінансів та бухгалтерії відповідає за працю:

– бухгалтерів;

– аудиторів;

– фінансових менеджерів.

Керівник відділу кадрів та управління персоналом відповідає за працю:

– HR-менеджерів;

– спеціалістів з підбору персоналу;

– працівників відділу кадрів.

Керівник відділу закупівель та логістики відповідає за працю:

– менеджерів з закупівлі сировини;

– спеціалістів з обліку запасів;

– логістів.

Керівник служби охорони відповідає за працю:

– охоронців.

1.3 Стислі відомості про технології збору та передачі інформації для об’єкта впровадження

Об'єктом впровадження є кондитерська фабрика “Житомирські ласощі”, яка знаходиться за адресою вул. Покровська, 67, місто Житомир, Україна. Також віддалений фірмовий магазин кондитерської фабрики який знаходиться за адресою вулиця Київська, 120, місто Житомир.

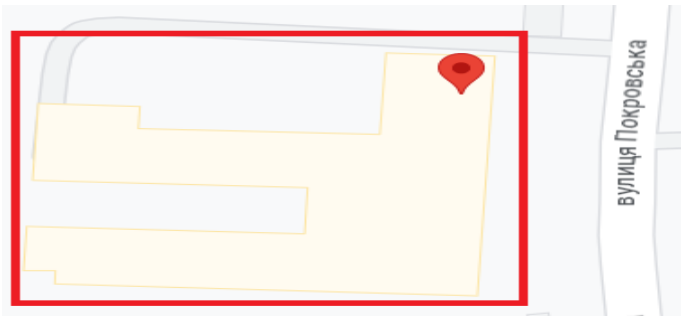

Рисунок 1.2 – Розташування об’єкта впровадження на карті.

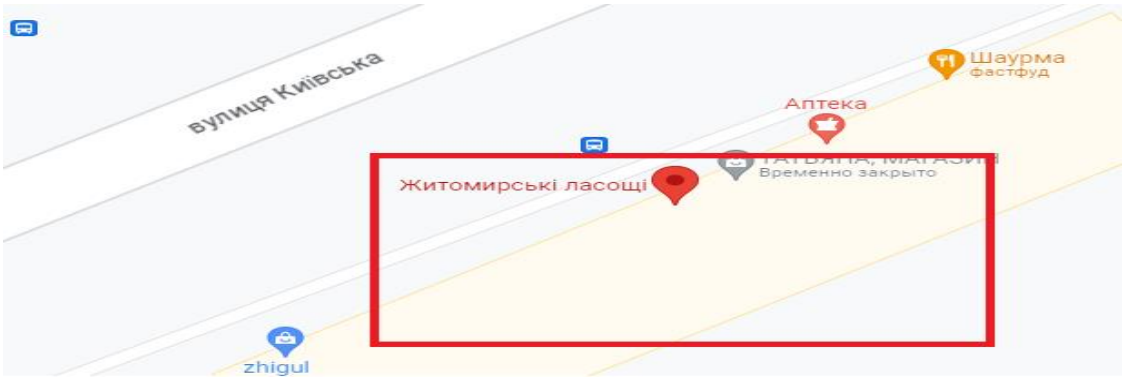

Рисунок 1.3 – Розташування віддаленого об’єкта на карті.

Всього на території кондитерської фабрики “Житомирські ласощі” знаходиться 4-х поверхова будівля, це головна будівля, де знаходиться вся комунікація та відділи.

Також 7 цехів для виробництва:

– цех виробництва печива – виготовлення різних видів печива;

– цех виробництва цукерок – виготовлення цукерок, шоколадних та кондитерських виробів;

– цех виробництва шоколаду – виробництво шоколаду, кондитерських виробів з шоколаду;

– цех виробництва вафель – виробництво вафельних виробів та вафельних трубочок;

– цех виробництва безцукрової продукції – виробництво продуктів для людей з діабетом;

– цех з упакування і фасування – упакування та фасування готових продуктів;

– цех зберігання готової продукції – зберігання готової продукції перед її відправкою.

Кондитерська фабрика “Житомирські ласощі” має власну їдальну для співробітників.

Два склади для зберігання готової продукції.

Будівлю для служби охорони, для забезпечення безпеки на території кондитерської фабрики.

Віддалений фірмовий магазин кондитерської фабрики “Житомирські ласощі”. Туди поставляють найсвіжіші товари з кондитерської фабрики без посередників.

Всі плани будівель зображені нижче. (рис. 1.4 – 1.16)

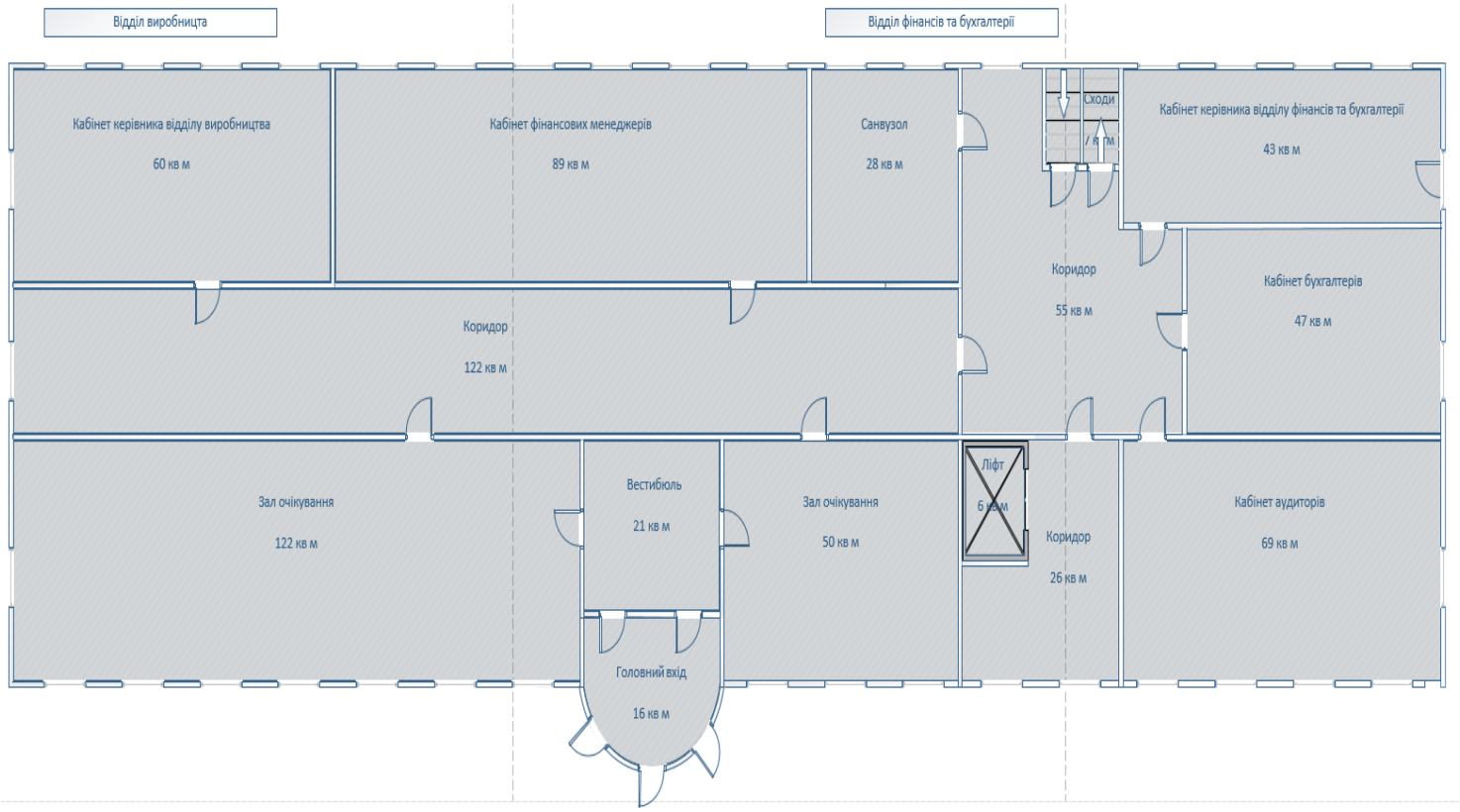

Рисунок 1.4 –Перший поверх головної будівлі кондитерської фабрики.

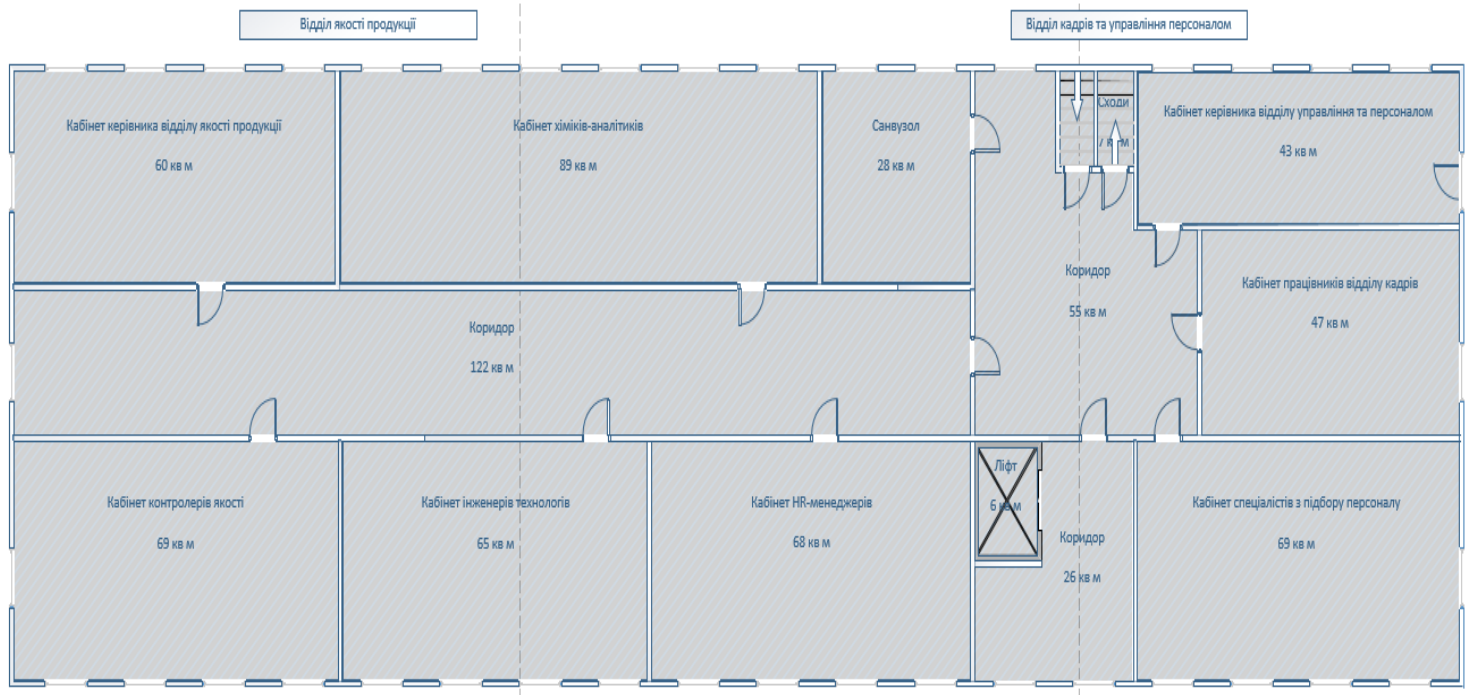

Рисунок 1.5 – Другий поверх головної будівлі кондитерської фабрики.

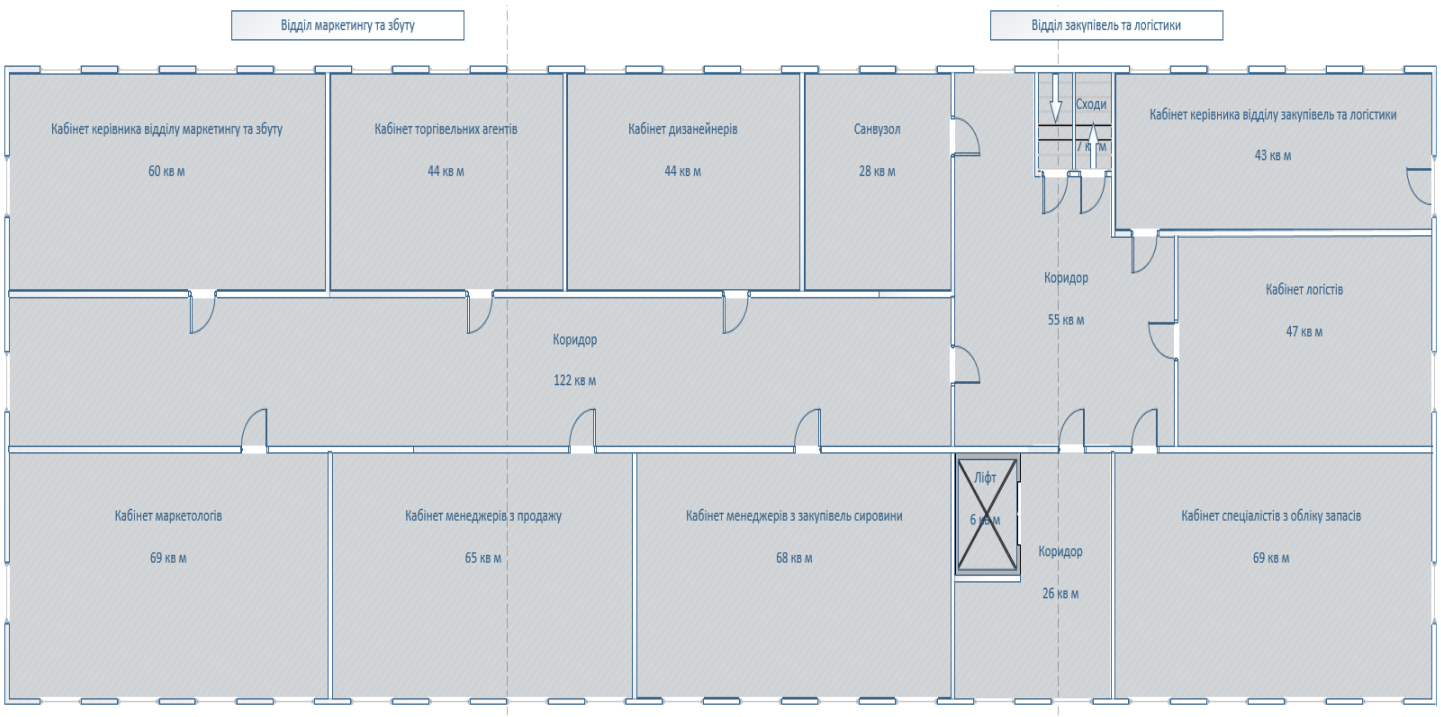

Рисунок 1.6 –Третій поверх головної будівлі кондитерської фабрики.

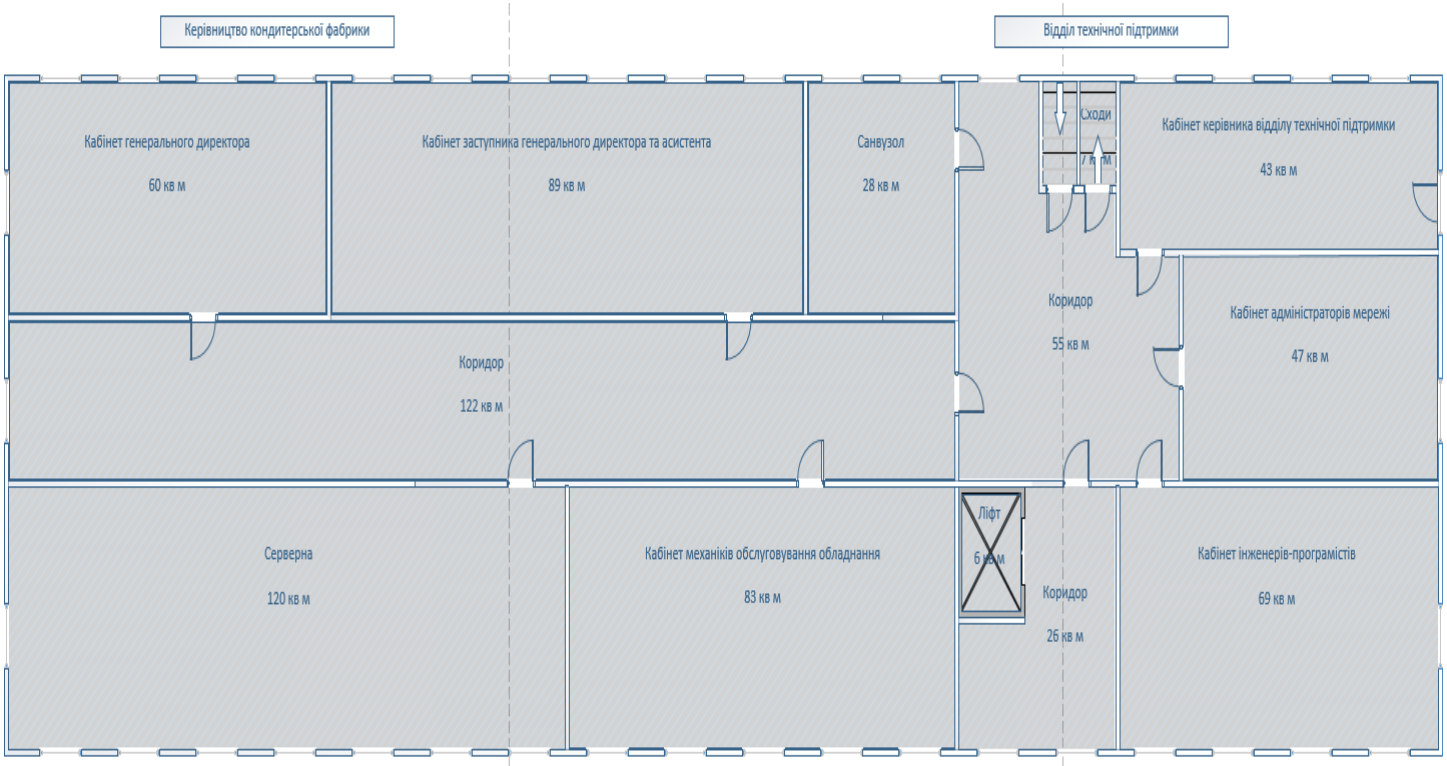

Рисунок 1.7 – Четвертий поверх головної будівлі кондитерської фабрики.

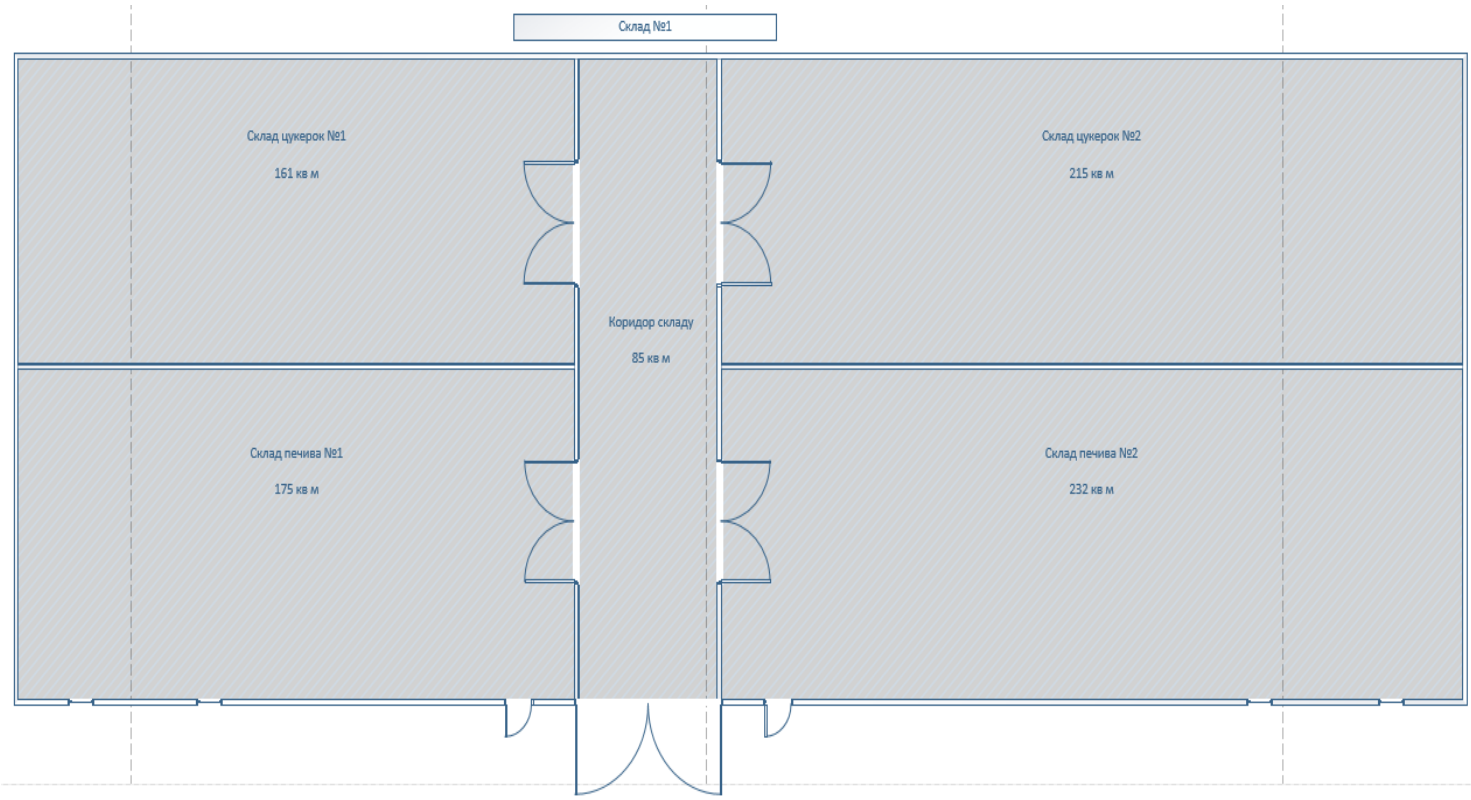

Рисунок 1.8 – Склад №1 кондитерської фабрики.

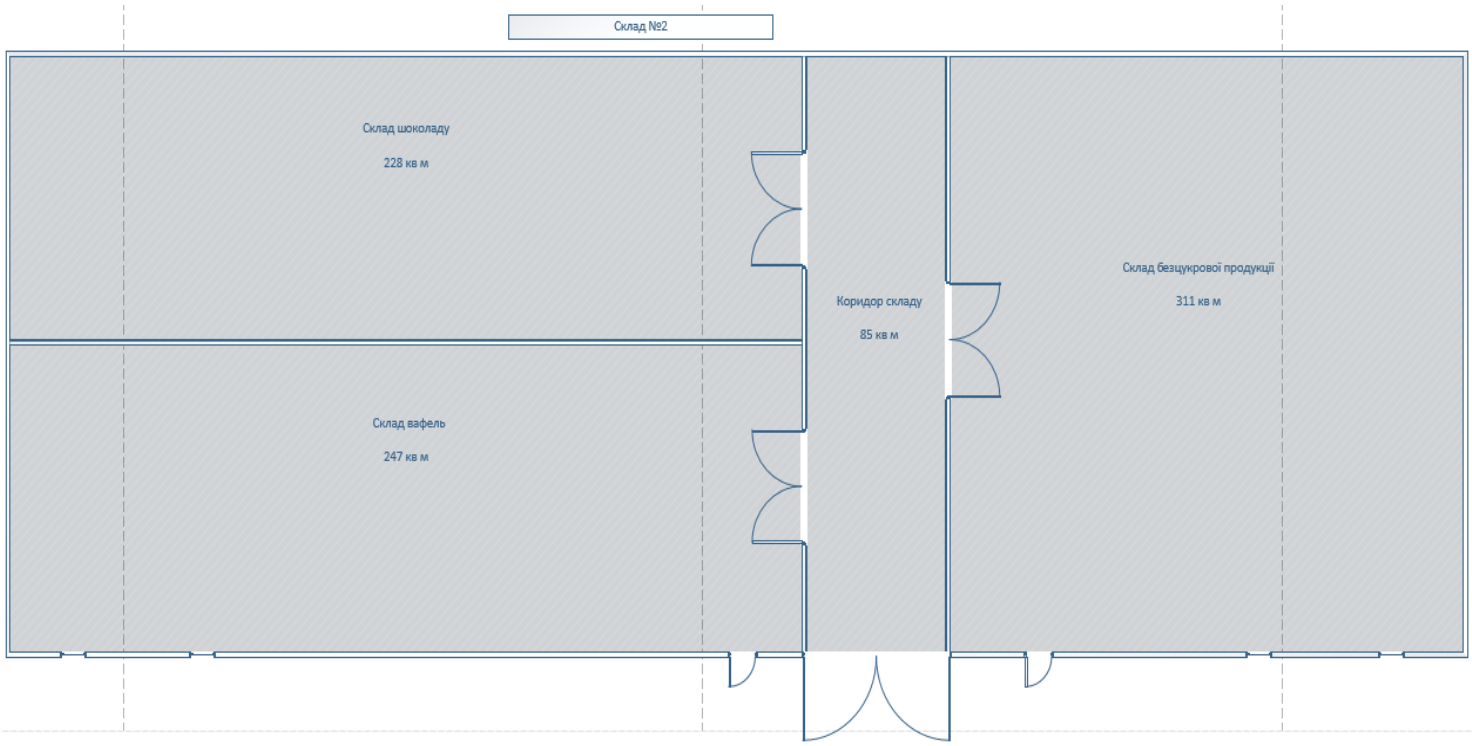

Рисунок 1.9 – Склад №2 кондитерської фабрики.

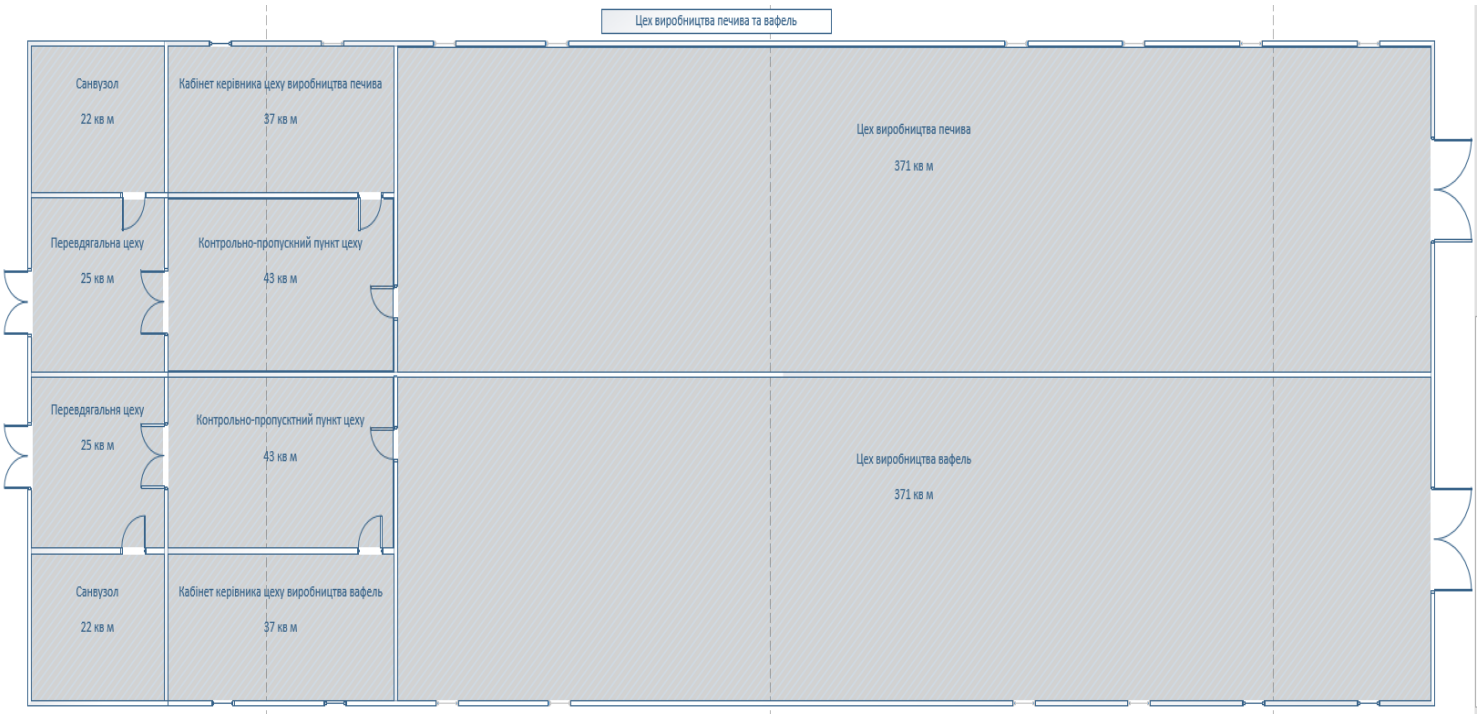

Рисунок 1.10 – Цех виробництва печива та вафель.

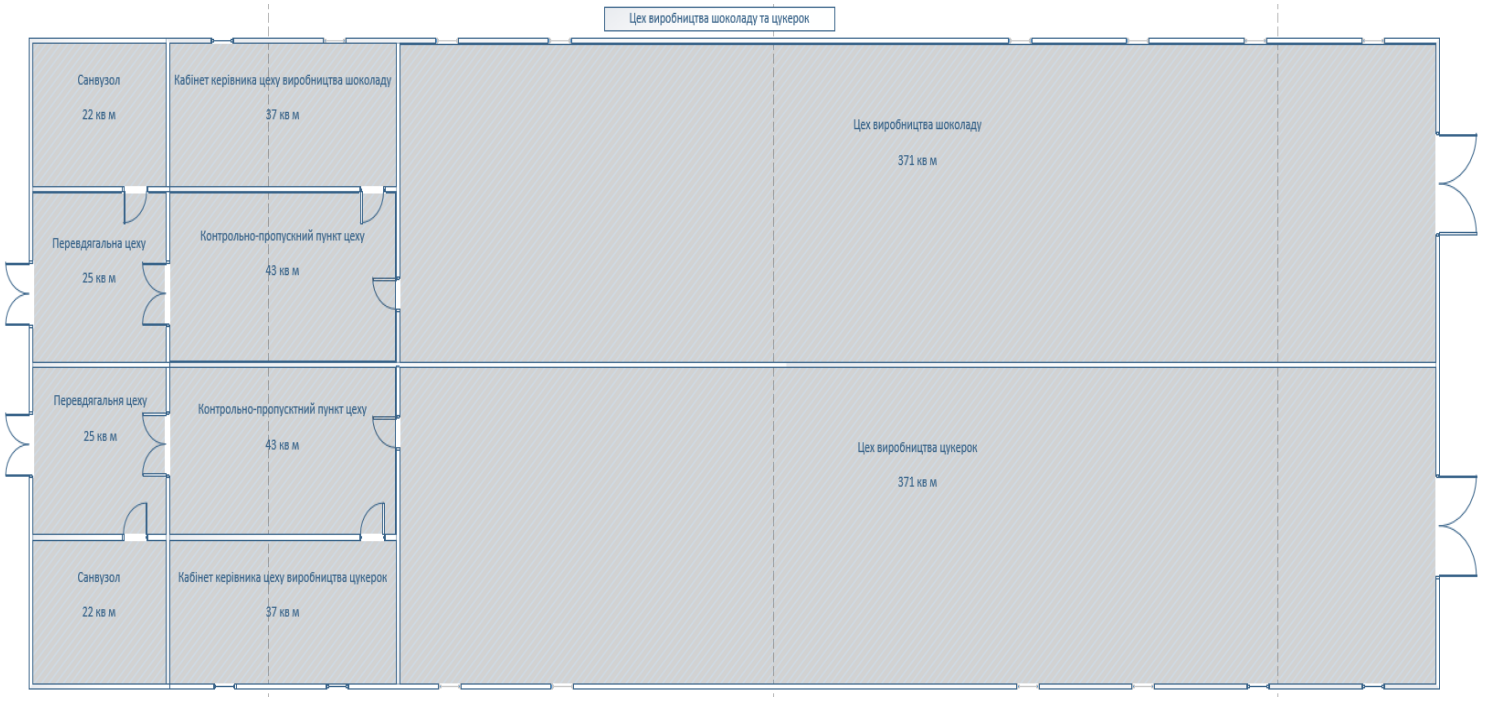

Рисунок 1.11 – Цех виробництва шоколаду та цукерок.

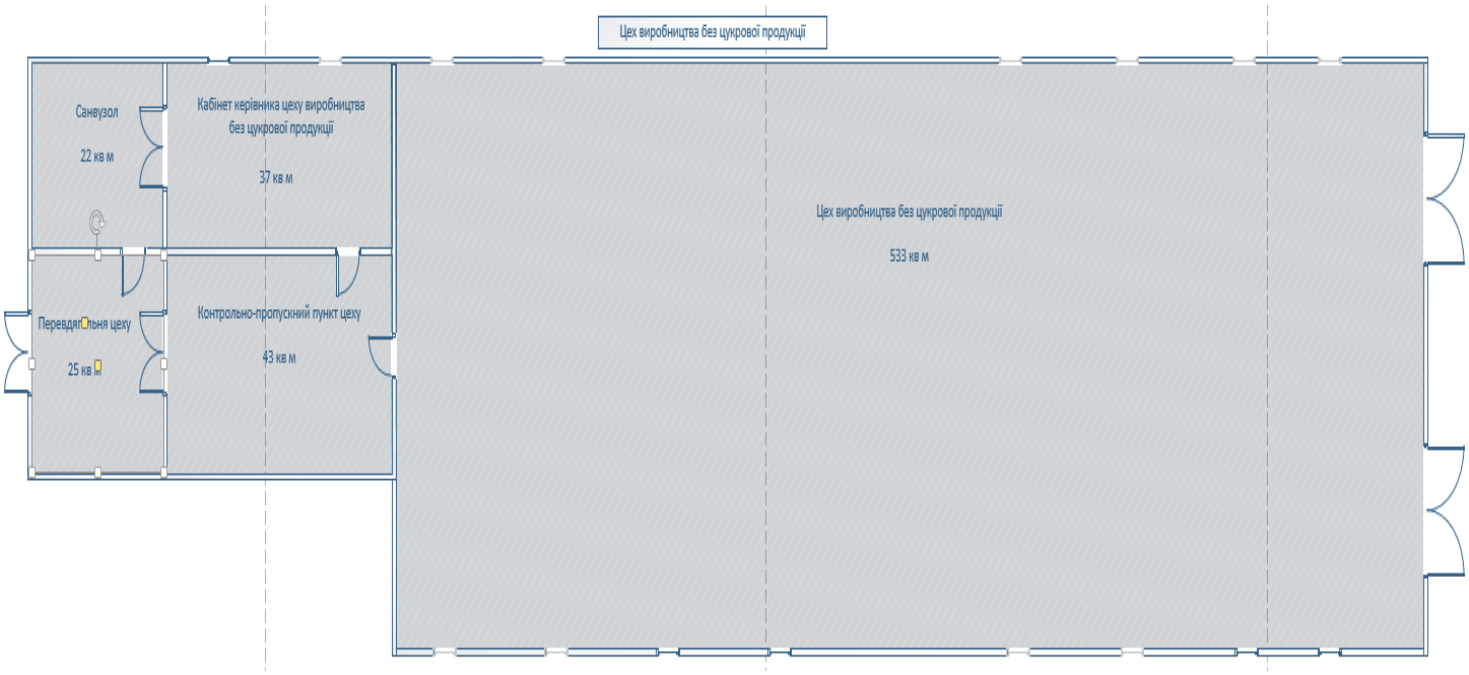

Рисунок 1.12 – Цех виробництва без цукрової продукції.

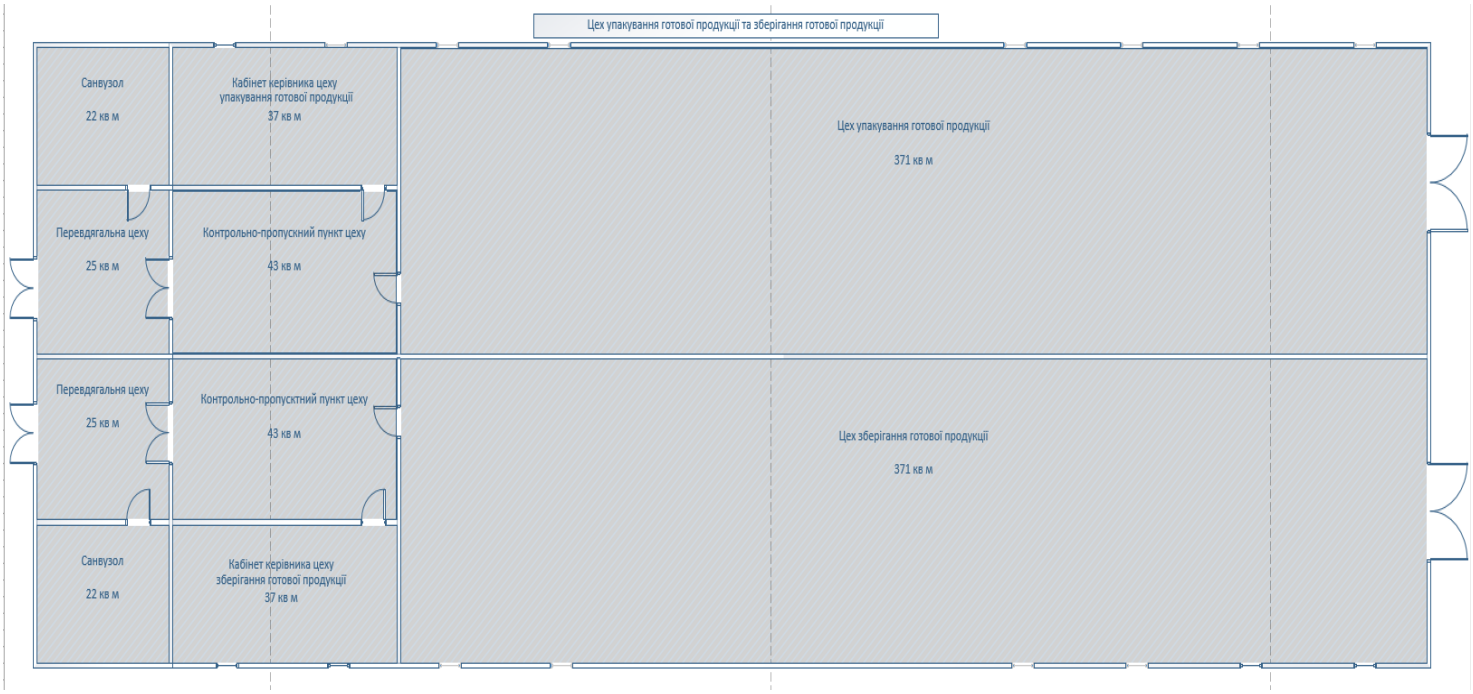

Рисунок 1.13 – Цех упакування готових продуктів та зберігання готової продукції.

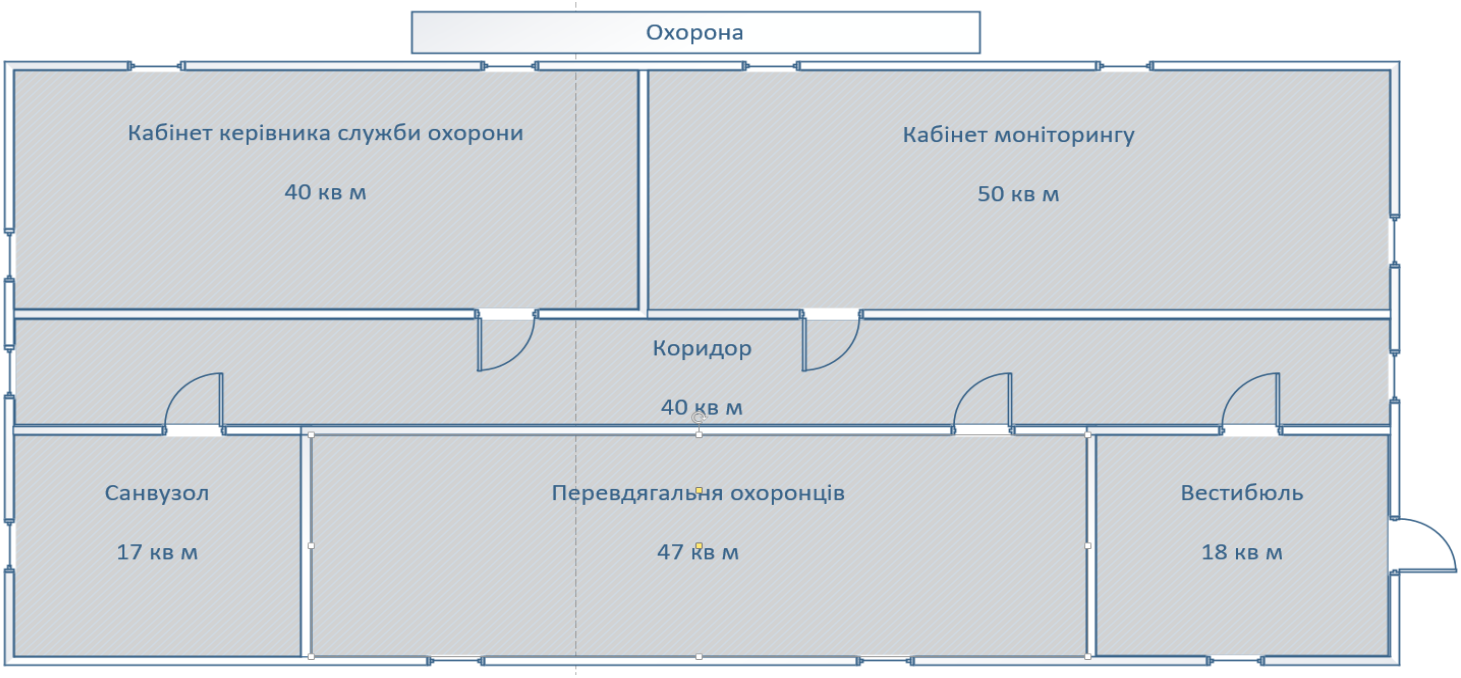

Рисунок 1.14 – Будівля охорони.

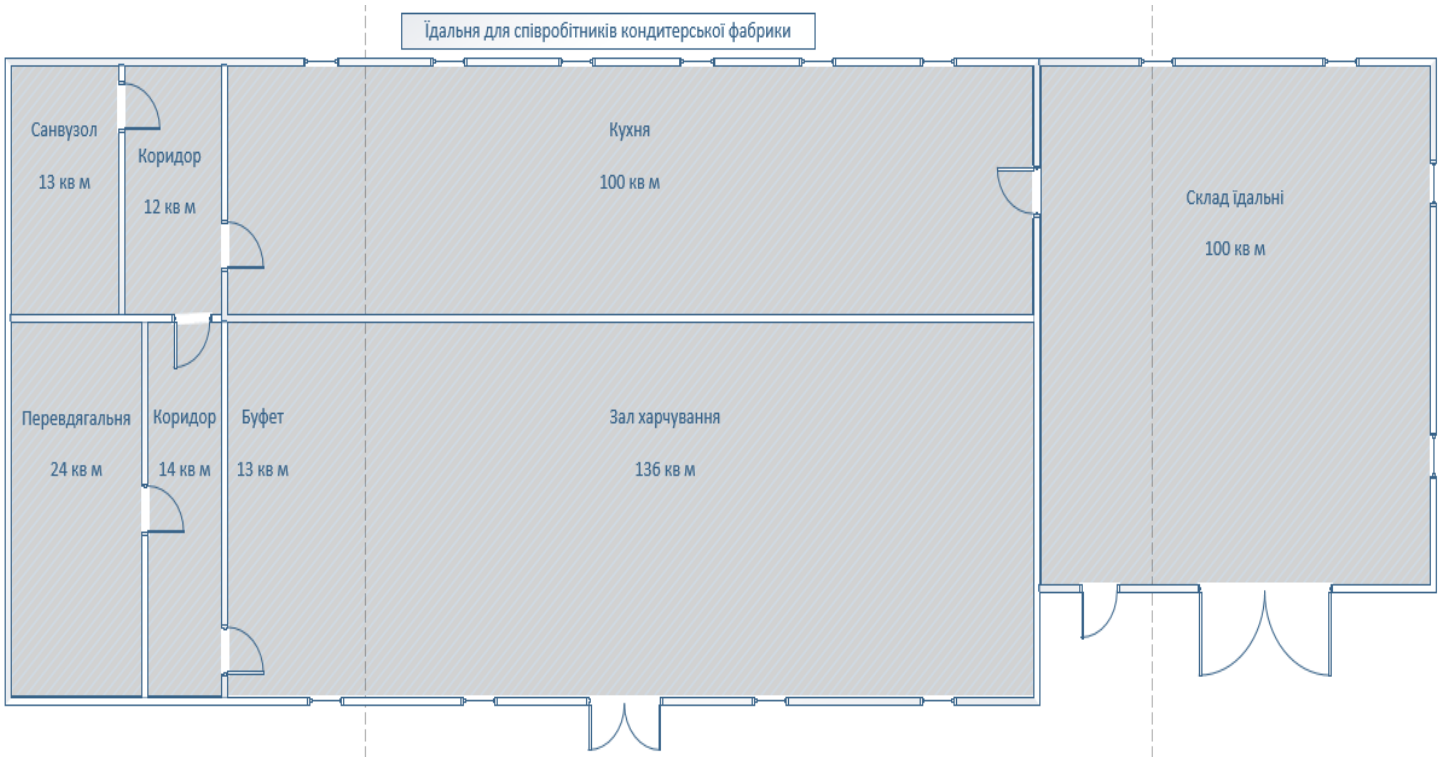

Рисунок 1.15 – Їдальня для співробітників кондитерської фабрики.

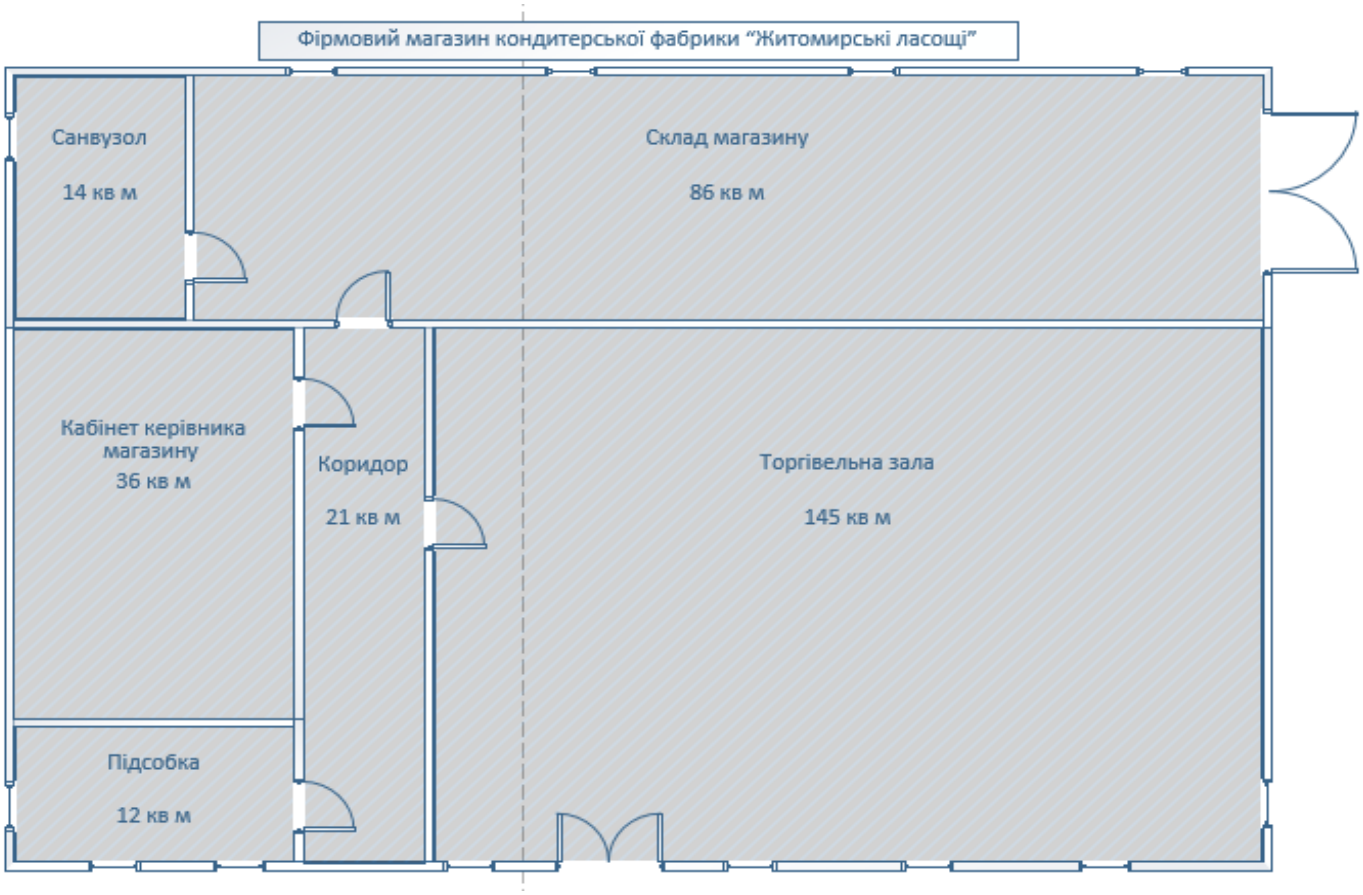

Рисунок 1.16 – Віддалений фірмовий магазин кондитерської фабрики.

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

Інформаційне забезпечення об'єкта впровадження кондитерської фабрики “Житомирські ласощі” включає в себе принципи, технічні засоби і способи, а також математичні методи, що допомагають забезпечити ефективну роботу фабрики та оптимізувати виробничі процеси. Нижче наведено загальний огляд цих аспектів:

Принципи інформаційного забезпечення:

– автоматизація: використання автоматизованих систем управління, обліку та контролю для забезпечення ефективної роботи фабрики.

– інтеграція: об'єднання різних компонентів інформаційної системи фабрики для забезпечення їх взаємодії та обміну даними.

– оптимізація: застосування методів та алгоритмів для покращення ефективності виробничих процесів, планування ресурсів та управління запасами.

Технічні засоби і способи інформаційного забезпечення:

– система автоматизованого управління складом: засоби інформаційного забезпечення для контролю запасів сировини, матеріалів та готової продукції на складі фабрики.

– електронна система управління якістю: впровадження системи керування якістю (наприклад, ISO 9001) з використанням електронних засобів для контролю якості продукції та процесів.

Математичні методи інформаційного забезпечення:

– статистичний аналіз: використання статистичних методів для аналізу даних про продукцію, якість, витрати, та інші показники для виявлення тенденцій, проблем та можливостей для вдосконалення процесів.

– оптимізаційні методи: використання оптимізаційних алгоритмів для вирішення задач планування виробництва, розподілу ресурсів, управління запасами та оптимального використання обладнання.

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

Інженерні рішення для інтелектуальної комп'ютерної системи контролю виробничих процесів в кондитерській фабриці є важливим кроком для підвищення якості та ефективності виробничих процесів.

У технологічному виробництві кондитерської продукції, системи автоматизації та контролю дозволяють забезпечувати додатковий рівень точності та контролю виробництва, а також допомагають у подальшому вдосконаленні процесів та оптимізації ресурсів.

Контроль вологості та температури виробничих приміщень є одним з найважливіших аспектів виробничого процесу у кондитерській фабриці. В

залежності від конкретного виду продукту та технології виробництва, температура та вологість можуть мати значний вплив на якість та характеристики продукту.

Для контролю вологості та температури зазвичай використовуються системи автоматичного регулювання, що дозволяють підтримувати необхідний рівень параметрів. Також використовуються датчики вологості та температури, які забезпечують постійний моніторинг у всіх розділах виробничого приміщення. Для регулювання рівня вологості та температури використовуються система контролю якості повітря.

Антиаварійні системи використовуються для контролю та попередження можливих аварій виробничого процесу. Для цього використовуються датчики, які моніторять рівень небезпечних параметрів, такі як температура та тиск, та автоматично вимикають або блокують виробничі лінії в разі виникнення небезпечних ситуацій.

Усі ці системи є важливими для забезпечення якості та безпеки виробничого процесу в кондитерській фабриці. Використання інженерних рішень для автоматизації та контролю виробничих процесів дозволяє знизити витрати та підвищити продуктивність виробництва.

1.6 Завдання і мета роботи

Головною метою кваліфікаційної роботи є оптимізація виробничих процесів, зменшення ризиків виробничих невдач та підвищення продуктивності в кондитерській фабриці “Житомирські Ласощі” завдяки інтелектуальної комп’ютерної системи контролю виробничих процесів. Для того що вирішити поставлену мету кваліфікаційної роботи, слід вирішити наступні завдання:

– визначення вимог до мережі: збір і аналіз потреб користувачів мережі та ресурсів, що мають бути доступні через мережу;

– вибір типу корпоративної мережі: провідна, бездротова або гібридна;

– визначення структури мережі: визначення топології, архітектури та маршрутизації корпоративної мережі мережі;

– вибір мережевого обладнання: вибір маршрутизаторів, комутаторів, мережевих адаптерів, точок доступу до бездротової мережі та іншого обладнання;

– возробка мережевої інфраструктури: налаштування мережевого обладнання, створення мережевих служб, налаштування захисту мережі.

Система повинна здійснювати автоматичний контроль показників виробничих процесів в режимі реального часу, збирати та обробляти потрібну інформацію для подальшого аналізу, моніторити експлуатаційні параметри та виявляти аварійні ситуації. Для забезпечення більшої ефективності та точності контролю, система має бути забезпечена датчиками, які вимірюють різні параметри виробничих процесів, відеомоніторами та іншими засобами автоматизації контролю.

Така автоматизована система контролю виробничих процесів дозволить підприємству забезпечити високу якість продукту, уникнути помилок під час виробництва та зменшити витрати на виробництво.

Також не слід забувати про віддалений фірмовий магазин кондитерської фабрики. Для нього буде зроблена віддалена мережа яка забезпечить чіткий контроль за запасами магазину, контроль за продажами.

Це рішення дуже добре вплине на віддалений фірмовий магазин, товари будуть доставлятись ще швидше, фінансова звітність буде набагато швидша. Також це вплине на покращення сервісу та задоволеності клієнтів, закази будуть оброблюватися набагато швидше та точне відстеження статусу замовлення.

Загалом, доєднання фірмового магазину до інтелектуальної комп'ютерної системи може мати значний позитивний вплив на бізнес, допомагаючи оптимізувати процеси та підвищити ефективність.

1.7 Визначення можливих напрямків рішення поставлених завдань

На сьогоднішній час кондитерська фабрика має звичайну примітивну топологію корпоративної мережі (рис. 1.17).

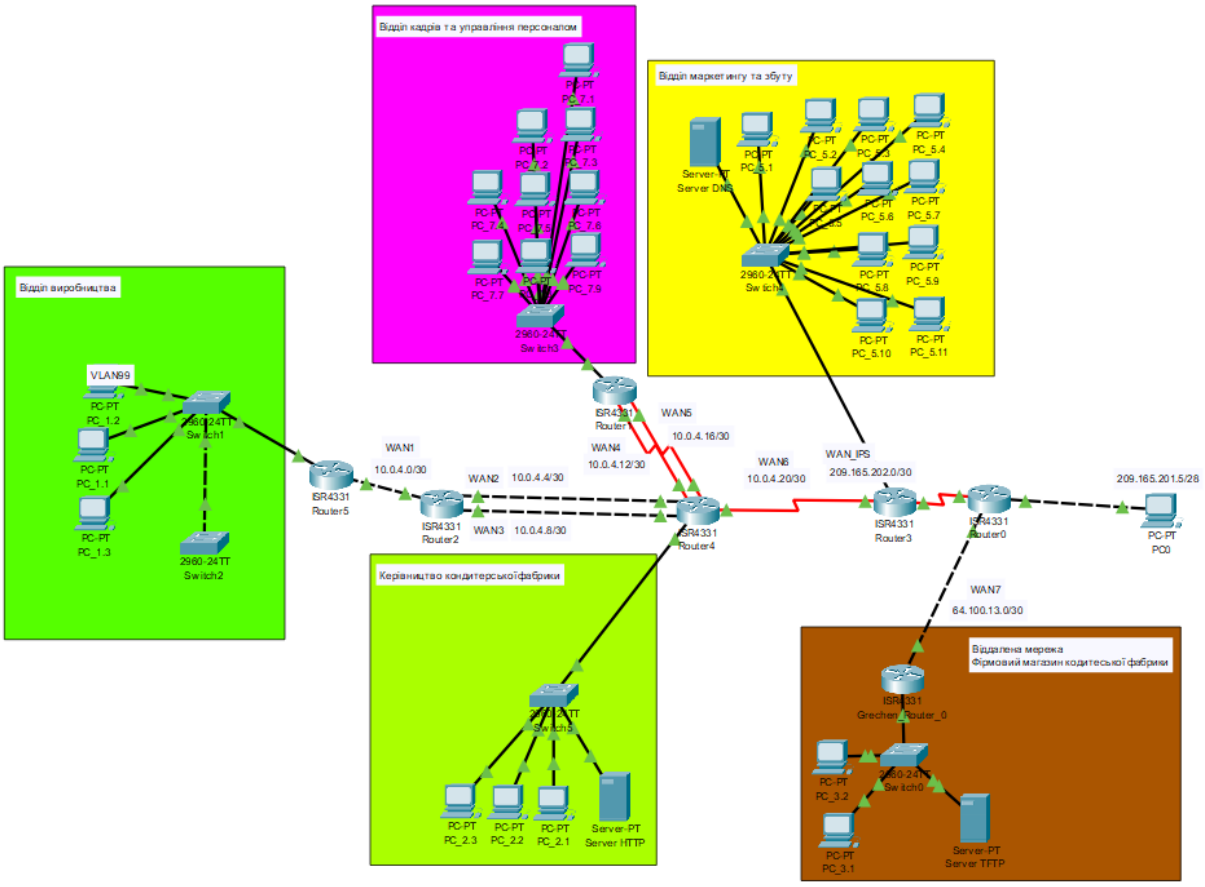

Рисунок 1.17 – Топологія мережі кондитерської фабрики “Житомирські Ласощі”

Корпоративна мережа кондитерської фабрики “Житомирські Ласощі” складається з 4 локальних під мереж та 1 віддаленої:

– «відділ виробництва»;

– «відділ керівництво кондитерської фабрики»;

– «відділ кадрів та управління персоналом»;

– «відділ маркетингу та збуду»;

– «віддалена мережа, магазин кондитерської фабрики».

Шляхом для вирішення поставної задачі потрібно буде:

Впровадження додаткових 4 локальних підмереж.

– «відділ технічної підтримки»;

– «відділ закупівель та логістики»;

– «відділ якості продукції»;

– «охорона».

Також «відділ виробництва» буде розподілений на 9 VLAN.

Кожен виробничий цех кондитерської фабрики буде облаштований:

– контрольно-пропускним пунктом з RFID турнікетом для контролю безпеки;

– інтелектуальною комп’ютерною системою контролю повітря в виробничих приміщення;

– анти пожежною системою для забезпеченню безпеки від пожеж;

– в кожному виробничому цеху, буде контролюватися рух виробничої лінії, для забезпечення швидкого технічного обслуговування у разі виникнення несправностей;

– кожен виробничий цех кондитерської фабрики буде обладнаний камерами відеоспостереження для забезпеченню контролю безпеки виробничих процесів.

Для взаємодії між пристроями буде використовуватися протокол CoAP. Це дуже простий та надійний протокол з підтримкою захисту DTLS.

Також модернізувати застаріле мережеве обладнання кондитерської фабрики на нове від компанії Cisco, це дуже відомий бренд який зарекомендував себе надійністю та репутацією.

Такі апгрейди для кондитерської фабрики мають багато плюсів та надійний захист інформації у мережі.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури та функціонування системи

Інтелектуальна комп'ютерна система контролю виробничих процесів в Житомирській кондитерській фабриці "Житомирскі Ласощі" на основі CoAP протоколу призначена для контролю виробничих процесів в цехах кондитерської фабрики для підвищення ефективності виготовлення продукції та оптимізації виробничих процесів. Інтелектуальна комп'ютерна система повинна забезпечувати моніторинг температури, вологості, диму та вмісту вуглекислого газу, щоб вчасно зреагувати на пожежу. Також на виробничих лініях будуть встановленні сенсори руху для слідкування постійного пересування продукції по ним та вчасно побачити технічну несправність у разі зупинки лінії та виконати певні дії. Для слідкуванням за роботою персоналу та стану приміщень, у цехи будуть встановленні камери для збору інформації.

Структура інтелектуальної комп'ютерної системи має складатись з наступних підмереж:

– «відділ виробництва», 250 вузлів;

– «відділ керівництво кондитерської фабрики», 38 вузлів;

– «віддалена мережа, магазин кондитерської фабрики», 100 вузлів;

– «відділ технічної підтримки», 61 вузлів;

– «відділ маркетингу та збуду», 39 вузлів;

– «відділ якості продукції», 50 вузлів;

– «відділ кадрів та управління персоналом», 67 вузлів;

– «відділ закупівель та логістики», 55 вузлів;

– «охорона», 35 вузлів.

Інтенсивність трафіку $\mu = 94$ (кадрів/с).

Блок адрес мережі − 172.23.72.0/21.

Для каналів між маршрутизаторами застосувати блок адрес 10.0.4.0/24

Середня довжина вихідного повідомлення в мережі − 650 байт.

Затримка передачі пакету в найбільшій мережі: «Відділ виробництва» − ≤ 6 мс.

− перший набір IP-адрес призначений інтерфейсам і підінтерфейсам маршрутизаторів у локальній мережі;

− другий набір IP-адрес призначається комутаторам у кожній локальній мережі;

− сервери налаштовані з IP-адресами, які обчислюються за правилом: IPадрес = перший можливий адрес у мережі + 9 + 4;

− останні доступні IP-адреси призначені вузлам;

− в під мережах VLAN використовується протокол DHCP для автоматичного призначення IP-адрес кінцевим пристроям.

Для функціонування комп'ютерної системи потрібно бути виконано базове налаштування маршрутизаторів, комутаторів, серверів та інших пристроїв за такими вимогами:

– надано унікальні ім'я пристроям;

– налаштовано пароль cisco на консолі та лінії vty;

– застосовано пароль class для привілейованого режиму;

– забезпечено шифрування усіх паролів;

− виконано налаштування банеру MOTD;

− налаштовано на лініях vty застосування протоколу ssh;

– назначено користувача 12320sk1_Grechen з паролем admincisco;

– використовуючи ім'я пристрою налаштовано ім'я домену та згенеровано ключ RSA завдовжки 1024 біт;

– встановлено значення тактової частоти 128000 на DCE-інтерфейсах маршрутизаторів;

− з використанням локальної бази було налаштовано аудит і відправку повідомлень про початок і завершення процесу exec.

Для ефективного та повноцінного функціонування система контролю виробничих процесів повинна мати певні налаштування.

Ситема повинна бути захищеною від несанціонованого доступу та має забезпечувати розширення у майбутньому для подальшого розвитку

2.1.1.2 Вимоги до чисельності та кваліфікації персоналу, який обслуговує систему і режим його роботи

Для забезпечення якісного обслуговування комп’ютерної системи, були сформовані такі вимоги до кваліфікації персоналу:

– керівник відділу технічної підтримки є магістром галузі "Комп’ютерна інженерія" з робочим досвідом від 2-3 років на даній посаді.

– інженери-програмісти мають бакалаврську освіту в галузі "Комп’ютерна інженерія". Вони відповідають за налагодження та підтримку працездатності мережі, зокрема, ремонт та налаштування мережевого обладнання.

– адміністратори мережі є молодшими спеціалістами в галузі "Комп’ютерна інженерія". Вони займаються налаштуванням та обслуговуванням комп’ютерів у мережі.

– механіки обслуговування обладнання мають бакалаврську або молодшу спеціалістську освіту в галузі "Автоматизація та комп’ютерно-інтегровані технології". Вони відповідають за моніторинг стану обладнання у цехах та, в разі несправності, проводять ремонт або заміну.

2.1.1.3 Вимоги до показників призначення

Інтелектуальна комп'ютерна система контролю виробничих процесів, реалізована на основі CoAP протоколу, призначена для використання в Житомирській кондитерській фабриці “Житомирські ласощі”

Вона повинна забезпечувати наступні показники призначення у наданні контролю, моніторингу та оптимізації виробничих процесів на фабриці.

Система здійснює контроль за різними аспектами виробництва, такими як температура, вологість, тиск, енергоспоживання та інші параметри, що впливають на якість та ефективність виробничого процесу.

Для комп’ютерної системи необхідно використовувати датчики, що відповідають таким вимогам:

– висока точність та швидкість вимірювання, щоб надати правдиву інформацію про вологість, температуру та задимленість. Точність вимірювання може бути в межах ±1% для вологості та ±0,5°C для температури;

– датчикі повинні постійно моніторити показники у робочих зонах цехів;

– конструкція датчиків повинна бути міцною, щоб витримувати умови робочих зон цехів кондитерської фабрики, такі як вібрації, удари та потенційні пошкодження;

– широкий діапазон робочих температур, наприклад, від -30°C до +60°C, щоб забезпечити надійну роботу як у холодних зимових умовах, так і в спекотному літньому кліматі;

– між датчиками та сервером для швидкої передачі даних буде встановлений зв’язок клієнт - сервер, такий зв’язок дозволяє зробити CoAP протокол.

Застосування CoAP протоколу дозволяє системі ефективно обмінюватися даними між різними пристроями та сенсорами, що використовуються на фабриці. Вона забезпечує швидку передачу інформації із зниженою споживанням енергії, що є важливим для оптимізації роботи системи.

2.1.1.4 Вимоги до надійності

Система повинна бути стійкою до відмов обладнання, програмних систем та електропостачання. Для забезпечення надійності комплексу

необхідно використовувати високонадійні апаратні компоненти, які повинні відповідати наступним критеріям:

– напрацювання на відмову - не менше 20000 годин;

– вірогідність безвідмовної роботи на період 100 годин має становити не менше 99,5%.

У нормальному режимі роботи мережа повинна забезпечувати швидкий обмін інформацією між кінцевими пристроями зі швидкістю не менше 2 Мб/с.

Вимоги до надійності системи повинні бути визначені для таких аварійних ситуацій:

– вихід з ладу апаратних компонентів системи, наприклад, маршрутизаторів і комутаторів, на період до 6 годин;

– відсутність електропостачання на період до 6 годин.

Необхідно забезпечити надійне збереження даних та їх захист від неправомірного впливу та нежаданих змін. Крім того, важливо забезпечити синхронізацію даних у випадках, коли створюються резервні копії.

Для забезпечення надійності роботи програмного забезпечення необхідно використовувати лише програмні продукти з відповідною ліцензією.

2.1.1.5 Вимоги до безпеки

Максимальне допустиме навантаження для серверних шаф повинно становити не менше 750 кг, а для телекомунікаційних шаф - не менше 450 кг.

В системі повинен бути передбачений доступ до загального заземлюючого електрода.

– в конструкції стелі не допускається використання фальш-панелей;

– каркас виробу повинен витримувати значні навантаження;

– всі елементи металевої конструкції мають бути заземлені;

– двері обов'язково повинні відкриватися назовні, без центрального упору та порогу, з огляду на техніку безпеки.

Розподільні шафи повинні бути заземлені за міжнародним стандартом ANSI/NECA/BICSI 568-2001 з використанням мідного провідника з площею перетину не менше 16,8 мм².

Комфортні умови праці для персоналу фабрики повинні відповідати санітарним нормам згідно з СанПіН 2.2.2/2.4.1340-03 “Гігієнічні вимоги до персональних електронних обчислювальних машин і організації роботи. Санітарно-епідеміологічні правила і нормативи”.

Рівень шуму і звукової потужності в зонах з персоналом, не повинні перевищувати вказаних значень, визначених ДЕСТом 12.1.003 ССБТ "Шум. Загальні вимоги безпеки" і санітарними нормами. При цьому слід враховувати рівні шуму і звукової потужності, створювані різними джерелами.

Для здійснення монтажу, налагодження, експлуатації, обслуговування та ремонту технічних засобів системи необхідно, щоб персонал мав відповідну документацію, підтверджуючу їх професійну кваліфікацію.

2.1.1.6 Вимоги по ергономіки та технічної естетики

Серверні шафи призначаються для комунікаційних вузлів і засобів підтримки, відповідно до встановлених стандартів. Рекомендується мати принаймні одну шафу для зберігання на кожному поверсі. Телекомунікаційні серверні шафи повинні відповідати вимогам стандарту (TIA-569-A):

– освітлення робочої зони шафи повинно бути на висоті 1 метра від підлоги і не менше 540 лк;

– рекомендується мати щонайменше 2 виділені розетки для живлення, які підключаються до окремого джерела живлення;

– двері шафи повинні відкриватися назовні, не мати центрального упору і порога. Розміри дверей: висота не менше 200 см, ширина - 91 см;

– конструкція шафи має забезпечувати легкий доступ до встановлених компонентів.

2.1.1.7 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню компонентів системи

Функціонування системи сплановане для неперервної роботи, з вимкненням відповідних сегментів для профілактичних робіт не частіше одного разу на рік. Інформація щодо видів, періодичності та регламенту обслуговування технічних засобів потрібно бути написано у спеціальних документах по експлуатації. Згідно з нормами, які встановлені ДЕСТом 21552-84 "Засоби обчислювальної техніки. Загальні технічні вимоги, правила приймання, методи випробувань, маркування, упаковка, транспортування і зберігання" і ДЕСТом 12.1.005-88 ССБТ "Загальні санітарно-гігієнічні вимоги до повітря робочої зони", приміщення, де розміщена обчислювальна техніка, повинні відповідати наступним умовам:

– температура навколишнього повітря має бути в межах (20 ± 5) °С;

– відносна вологість навколишнього повітря повинна бути (60 ± 15)%;

– атмосферний тиск має бути від 84 до 107 кПа (680-800 мм рт. ст.);

– запиленість повітря в приміщенні не повинна перевищувати 1 мг/куб. м з розміром часток не більше 3 мкм;

– напруженість зовнішнього електричного поля не повинна перевищувати 0.3 V/m;

– напруженість зовнішнього магнітного поля не повинна перевищувати 5.0 А/м;

– частота вібрацій не повинна перевищувати 25 Гц з амплітудою зсуву не більше 0.1 мм.

У приміщенні не повинно бути агресивних речовин, які можуть спричинити корозію. Температура, вологість та атмосферний тиск в приміщеннях, де працює оперативний та обслуговуючий персонал, повинні

бути контрольовані. Змінна напруга повинна проходити через фільтри для приглушення перешкод.

Допустиме усталене відхилення напруги на висновках приймачів електричної енергії складає ±5% від номінальної напруги електричної мережі, згідно з ДЕСТом 21128 (номінальна напруга).

Поточне значення напруги повинно бути 220V ± 5% (максимально ± 10%), частота - 50 ± 0,2 Гц (максимально ± 0,4 Гц), коефіцієнт несинусоїдальності - до 8% в межах норми і до 12% як максимум (згідно з ДЕСТом 13109-97).

Обладнання комп'ютерної системи повинно бути комплектоване ЗІП на весь гарантійний термін. Комплект ЗІП повинен поповнюватися протягом усього періоду експлуатації системи відповідно до умов договору на сервісне обслуговування.

2.1.1.8 Вимоги до захисту інформації від несанкціонованого доступу

Для забезпечення захисту інформації, яка обробляється в різних системах рівня і призначення, необхідно використовувати комплекс заходів організаційного, програмного, криптографічного характеру. Ці заходи спрямовані на захист інформації під час її автоматизованої обробки, зберігання та передачі через комунікаційні канали.

Загальні та основні напрями захисту інформації такі:

– захист від несанкціонованого доступу та спеціальних впливів, що можуть призвести до розкрадання, втрати, витоку, знищення, спотворення або підробки інформації;

– захист від технічного витоку інформації під час її обробки, зберігання та передачі через комунікаційні канали.

Для забезпечення ефективного захисту інформації рекомендуються такі заходи:

– створення документального переліку конфіденційної інформації з урахуванням особливостей відповідного відомства або галузі;

– спровадження системи контролю доступу, яка обмежує права використання інформації для виконавців (користувачів, обслуговуючого персоналу) і пов'язаних з нею робіт і документів;

– обмеження доступу персоналу та сторонніх осіб до приміщень, де знаходяться системи інформатизації та зберігаються інформаційні носії.

– розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів та захисних засобів;

– реєстрація дій користувачів і обслуговуючого персоналу комп'ютерної системи та контроль їх дій, а також дій сторонніх осіб;

– ефективне управління машинними носіями інформації, ключами та ключовою документацією для запобігання їх розкраданню, підміні або знищенню;

– використання технічних засобів, що відповідають стандартам електромагнітної сумісності;

– використання сертифікованих засобів захисту інформації;

– використання захищених каналів зв'язку і криптографічних засобів захисту інформації;

– організація фізичного захисту приміщень і технічних засобів за допомогою охоронних сил і технічних засобів, що ускладнюють незаконне проникнення, крадіжку документів, інформаційних носіїв та засобів інформатизації, а також запобігають проникненню шпигунської або розвідувальної техніки.

Особи, які мають доступ до конфіденційної інформації, відповідають за дотримання процедур забезпечення її захисту, встановлених установою або підприємством.

2.1.1.9 Вимоги до схоронності інформації при аваріях

У разі виникнення аварійних ситуацій, система повинна бути добре захищеною, щоб гарантувати безперебійну роботу і збереження накопичених даних. Для досягнення цієї мети, будуть застосовуватися такі вимоги:

– резервне живлення: встановлення систем резервного живлення, таких як резервні джерела живлення або безперебійні джерела живлення (UPS), для забезпечення електроживлення в разі відмови основного джерела. Резервне живлення буде працювати 24 години, цього часу буде достатньо щоб вирішити технічні питання;

– резервне копіювання: регулярне створення резервних копій накопиченої інформації і зберігання їх на надійних носіях, щоб в разі аварії мати можливість відновити дані. Збереження інформації відбувається зразу як вона надходить на сервер, записи з відеокамер у робочих зонах, мають зберігатися 6 місяці, дані з датчиків 3 місяці, також такі дані мають мати 1 резервну копію, така копія створюється кожні 24 години на іншому сервері в разі виходу з ладу серверу зберігання. Резервні копій даних зберігаються такий же тривалий час як і звичайні дані;

– механізми автоматичного відновлення: використання спеціальних програмних механізмів, які дозволяють автоматично відновлювати роботу системи після відновлення живлення або усунення несправностей. Гранична затримка на відновлення усіх компонентів у робочий стан приблизно 4 години, разом з тестуванням роботи системи після відновлення. Але це залежить від багатьох факторів. Бо на заміну пошкоджених компонентів апаратного забезпечення може виникнути більше часу.

2.1.1.10 Вимоги до патентної чистоти

Розробка комп'ютерної системи, яка не призначена для експорту, не обмежена патентними вимогами. Проте, важливо зазначити, що авторські права виробників обладнання системи та розробники програмного

забезпечення підпадають під захист не лише міжнародного, але й українського законодавства. Тому, як комплексне обладнання, так і окремі його компоненти, включаючи програмне забезпечення, можуть бути використані лише згідно з умовами, визначеними у договорах з генпідрядником, постачальником системного обладнання або розробником комп'ютерної системи. Передача цих матеріалів третім особам без попередньої письмової згоди відповідних сторін є забороненою та недопустимою.

2.1.1.11 Вимоги до стандартизації й уніфікації

При розробці комп'ютерної системи необхідно забезпечити її універсальність і можливість розширення в майбутньому.

Усі компоненти, що входять до складу системи, мають відповідати міжнародним стандартам. Система повинна відповідати світовим стандартам у створенні комп'ютерних систем, щодо їх функціонального розвитку, зручності в експлуатації та обслуговуванні. Вимоги до функцій, які виконує комп’терної системи.

2.1.2 Вимоги до функцій, які виконує комп’ютерна система

2.1.2.1 Перелік функцій та задач

Основні функції та задачі системи включають:

– система забезпечує збір і моніторинг даних з різних датчиків та пристроїв, що використовуються в процесі виробництва. Це можуть бути дані про температуру, вологість, рівень запасів сировини, параметри обладнання тощо;

– система виконує аналіз зібраних даних та визначає ключові показники продуктивності, такі як ефективність виробничих ліній, втрати часу, якість вироблених продуктів тощо. Це дозволяє виявляти потенційні проблеми та покращувати продуктивність фабрики;

– система моніторить роботу обладнання та виробничих процесів і надає можливість реагувати на аварійні ситуації або несправності. Наприклад, вона може автоматично сповіщати операторів про виникнення проблем та надавати рекомендації щодо вирішення;

– система дозволяє здійснювати віддалений моніторинг та управління виробничими процесами. Оператори можуть відстежувати стан процесів, контролювати параметри та виконувати необхідні дії з віддаленої робочої станції;

– система контролює параметри безпеки виробничого середовища, виявляє потенційні загрози та сповіщає про них. Вона може допомагати в управлінні ризиками та забезпеченні безпеки працівників.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення

Основні вимоги до інформаційного забезпечення включають:

– система повинна забезпечувати конфіденційність, цілісність та доступність інформації, що обробляється в процесі контролю виробничих процесів. Реалізація механізмів аутентифікації, авторизації та шифрування може бути використана для забезпечення цих вимог.

– інформаційна система повинна бути стійкою до відмов і збоїв, а також здатною відновлюватися після непередбачуваних ситуацій. Запобігання втраті даних та резервне копіювання можуть бути використані для забезпечення надійності системи;

– система повинна забезпечувати ефективну передачу та обробку інформації для забезпечення безперебійної роботи виробничих процесів. Оптимізація мережевої пропускної здатності та швидкодії обробки даних можуть бути використані для досягнення цієї вимоги;

– система повинна бути гнучкою та здатною масштабуватися залежно від зростання потреб виробничих процесів. Архітектурні рішення, що

дозволяють розширювати обсяги інформації та кількість пристроїв, можуть бути використані для досягнення цієї вимоги;

– система повинна бути сумісною з існуючими технологіями та стандартами, що застосовуються на Житомирській кондитерській фабриці "ЖЛ". Це забезпечить інтеграцію з існуючою інфраструктурою та легкість взаємодії з іншими системами;

– система повинна мати зручний та ефективний інтерфейс для керування та моніторингу виробничими процесами. Розробка інтуїтивно зрозумілих інструментів управління та відображення стану системи може бути використана для досягнення цієї вимоги.

2.1.3.2 Вимоги до лінгвістичного забезпечення

Основні вимоги до лінгвістичного забезпечення включають:

– система повинна мати можливість працювати з різними мовами, включаючи національні мови та мови, що використовуються на фабриці. Це вимагає наявності відповідних мовних ресурсів, словників, граматик та алгоритмів для обробки тексту в різних мовах;

– система повинна мати здатність аналізувати текстову інформацію, включаючи розпізнавання та виділення ключових слів, виявлення синтаксичних залежностей та семантичний аналіз. Це допомагає системі зрозуміти зміст тексту та виконувати відповідні дії на основі отриманої інформації.

2.1.3.3 Вимоги до технічного забезпечення

Основні вимоги до технічного забезпечення включають:

Маршрутизатори обов’язково мають бути здатні підтримувати віртуальні локальні мережі (VLAN) та використовувати маршрутизаційний протокол OSPF. Також вони повинні мати для розширення модулі, які дозволяють додавати серійні порти. У шлюзових маршрутизаторах також має бути підтримка віртуальних приватних мереж (VPN).

Щодо комутаторів, вони повинні мати здатність підтримувати віртуальні локальні мережі і мати не менше 24 портів Fast Ethernet. Особливістю комутаторів, що використовуються в підмережі паркінгу, є наявність портів Fast Ethernet, які підтримують технологію передачі енергії через Ethernet (PoE).

Маршрутизатори та комутатори повинні бути фірми Cisco, всі інші пристрої будь якої фірми але належної якості та функціональності, головне щоб підходили по технічним характеристикам для використання у комп’ютерній системі

Додаткові технічні вимоги:

– технічне забезпечення системи повинно бути надійним та стабільним, забезпечуючи безперебійну роботу системи протягом тривалого часу. Це включає високу стійкість до відмов, захист від перебоїв живлення, а також можливість відновлення роботи системи після аварійних ситуацій;

– технічне забезпечення повинно забезпечувати оптимальну швидкодію обміну даними та обробки інформації. Це може включати використання потужних процесорів, швидкодійних комунікаційних інтерфейсів та оптимізованих алгоритмів обробки даних;

– технічне забезпечення повинно бути сумісним з використовуваними пристроями та системами у виробничому середовищі. Це включає підтримку стандартних протоколів зв'язку, інтерфейсів та форматів даних, що використовуються на фабриці;

– технічне забезпечення повинно мати вбудовані механізми захисту від несанкціонованого доступу, злому та витоку конфіденційної інформації. Це включає використання шифрування даних, механізмів аутентифікації та контролю доступу до системи;

– технічне забезпечення повинно мати можливість масштабування для відповіді на зростаючі потреби виробничих процесів. Це може включати гнучку архітектуру, розширення обчислювальних ресурсів та підтримку розподіленого обробки даних;

– технічне забезпечення повинно мати належну технічну підтримку, включаючи можливість отримання консультацій, вирішення проблем та оновлення програмного та апаратного забезпечення.

2.1.3.4 Вимоги до організаційного забезпечення

Основні вимоги до організаційного забезпечення включають:

– організаційна структура системи повинна бути чітко визначена і забезпечувати ефективну координацію між різними підрозділами та відповідальними особами. Це може включати формування команди проекту, призначення відповідальних за різні аспекти системи та встановлення чітких ліній комунікації;

– організаційне забезпечення повинно забезпечувати належні ресурси, які включають фінансові, технічні та людські ресурси. Необхідний персонал повинен мати необхідні навички та знання для ефективної роботи з системою;

– організаційне забезпечення повинно передбачати навчання та тренінг для персоналу, який буде використовувати та керувати системою. Це допоможе забезпечити належне розуміння функцій системи та оптимальне використання її можливостей;

– організаційна структура повинна мати механізми для управління змінами в системі. Це включає процеси оновлення та модернізації системи, а також вирішення проблем та змін у вимогах користувачів;

– організаційне забезпечення повинно включати заходи для забезпечення безпеки та конфіденційності інформації, яка обробляється системою. Це може включати впровадження захисту даних, контроль доступу та моніторинг безпекових заходів;

– організаційне забезпечення повинно передбачати механізми для супроводження та підтримки системи протягом її життєвого циклу. Це включає надання технічної підтримки, вирішення проблем та регулярне оновлення системи;

2.1.3.5 Вимоги до методичного забезпечення

Основні вимоги до методичного забезпечення включають:

– методичне забезпечення повинно містити докладні інструкції зі встановлення, налаштування та початкового запуску системи. Це допоможе персоналу фабрики впровадити систему належним чином і забезпечити її коректну роботу;

– методичне забезпечення повинно містити розширені руководства користувача, які охоплюють різні аспекти використання системи. Це може включати опис функцій та можливостей системи, процедури роботи з інтерфейсом, аналіз даних та генерацію звітів;

– методичне забезпечення повинно включати детальну технічну документацію, яка описує архітектуру системи, протоколи комунікації, структуру бази даних та інші технічні аспекти. Це допоможе технічному персоналу зрозуміти систему з точки зору її розробки та технічної підтримки;

– методичне забезпечення може включати навчальні матеріали, такі як презентації, тренінги або відеоуроки, які допоможуть персоналу фабрики освоїти роботу з системою та використовувати її на практиці;

– методичне забезпечення повинно містити поради щодо усунення найпоширеніших несправностей або проблем, які можуть виникнути під час експлуатації системи. Це допоможе персоналу швидко вирішувати технічні проблеми та забезпечувати неперервну роботу системи.

2.2 Розробка загальної структурної схеми

Інтелектуальна комп'ютерна система контролю виробничих процесів в Житомирській кондитерській фабриці "Житомирскі Ласощі" базується на CoAP протоколі та складається з різних ключових компонентів. Сервери виступають як центральні обчислювальні вузли, які забезпечують надання ресурсів та послуг іншим комп'ютерам у мережі. Вони здійснюють

централізоване зберігання даних, обробку та передачу інформації, а також виконання спеціалізованих завдань.

Окрім серверів, важливою складовою системи є клієнтські комп'ютери або робочі станції, які виступають терміналами, через які користувачі отримують доступ до ресурсів та послуг, що надаються серверами. Вони забезпечують зручний та ефективний спосіб взаємодії з комп'ютерною системою.

Додатковою складовою мережевої інфраструктури є мережеве обладнання, яке включає комутатори, маршрутизатори та мережеві контролери. Ці компоненти забезпечують з'єднання та комунікацію між різними елементами мережі, створюючи надійну та ефективну інфраструктуру.

У кондитерській фабриці “Житомирські Ласощі” розглядається структурна схема комплексу технічних засобів комп'ютерної системи, де рівень ядра та розподіл мережі будуть поєднуватися за допомогою маршрутизаторів комп’ютерної системи.

Такий підхід дозволяє безпосередньо передавати дані від кожного комутатора до призначених отримувачів, покращуючи продуктивність та забезпечуючи високий рівень безпеки мережі. Така архітектура гарантує, що дані не обробляються на непризначених сегментах мережі, забезпечуючи ефективну та безпечну передачу інформації.

Розроблену структурну схему наведено на рисунку 2.1.

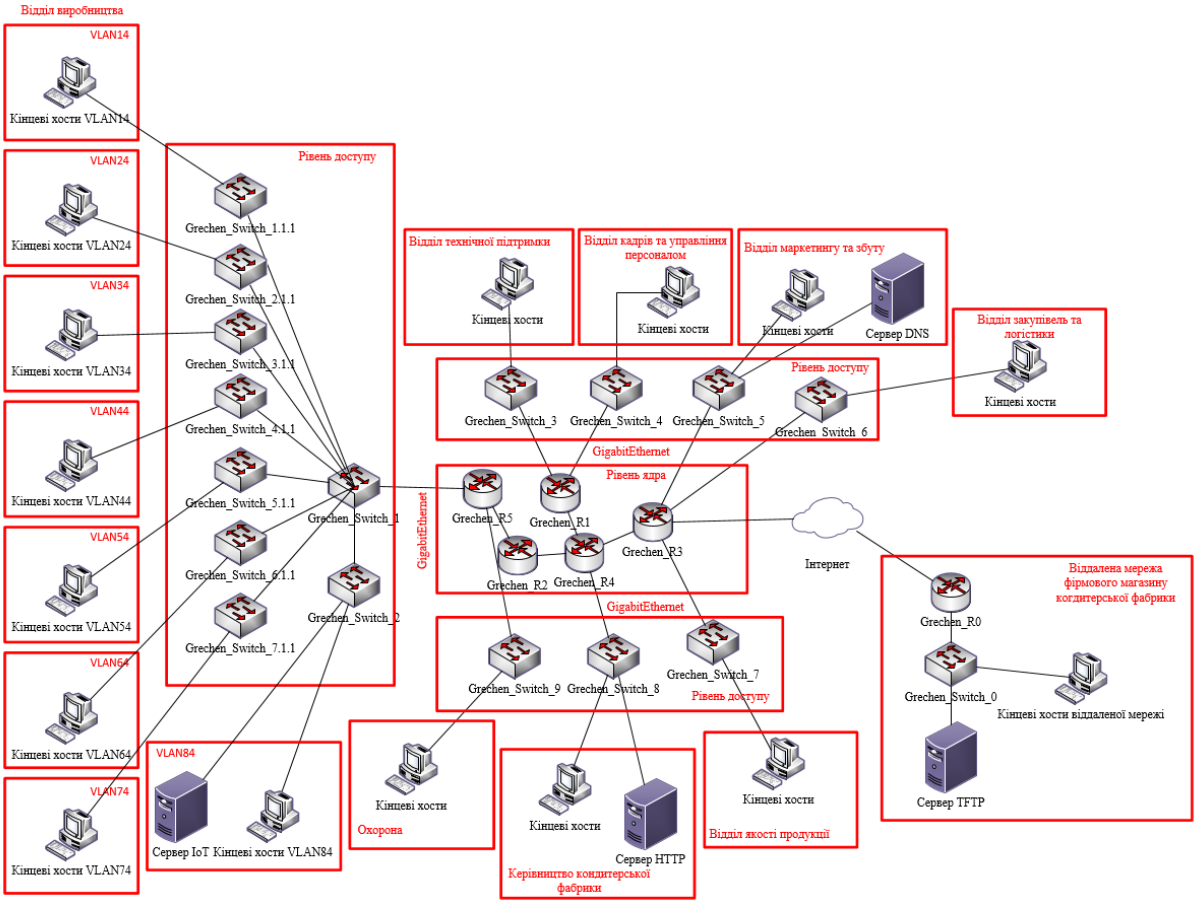

Рисунок 2.1 – Структурна схема інтелектуальної комп’ютерної системи кондитерської фабрики “Житомирські ласощі”

2.3 Розробка специфікації апаратних засобів комп’ютерної системи

Для побудови корпоративної мережі кондитерської фабрики “Житомирські Ласощі” були використані маршрутизатори та комутатори фірми Cisco, а саме:

Маршрутизатор Cisco ISR 4451-X є потужним пристроєм з серії Integrated Services Router (ISR), спеціально розробленим для організацій з великими потребами в мережевих послугах. Він пропонує високу продуктивність, масштабованість та надійність.

Основні характеристики маршрутизатора Cisco ISR 4451-X включають:

– маршрутизатор підтримує високі швидкості передачі даних, здатний обробляти трафік зі швидкістю від 1 до 2 Gbps залежно від конфігурації. Він забезпечує велику пропускну здатність, що робить його ідеальним для великих мереж з високим обсягом даних;

– маршрутизатор має модульну архітектуру, що дозволяє легко розширювати його можливості. Він підтримує різні модулі і інтерфейси, такі як порти Gigabit Ethernet, порти 10 Gigabit Ethernet, WAN-інтерфейси, включаючи T1/E1, T3/E3, а також модулі для розширення функціональності маршрутизатора.

– ISR 4451-X має розширені можливості для інтегрованих сервісів. Він підтримує такі функції, як маршрутизація, комутація, вогнева стіна, VPN, безпека, QoS, управління мережею та інші. Це дозволяє вам реалізувати різноманітні послуги і функції в одному пристрої;

– маршрутизатор має вбудовану резервування та захист від відмов, такі як модуль Hot Standby Router Protocol (HSRP), що забезпечують неперервну роботу мережі. Він також підтримує функції віддаленого резервного копіювання та відновлення для забезпечення безперебійної роботи мережі в разі аварії.

Повні технічні характеристики маршрутизатора Cisco ISR 4451-X:

– продуктивність маршрутизації: До 1 Гбіт/сек;

– продуктивність пропускання трафіку: До 2 Гбіт/сек ;
(двосторонній режим);

– кількість портів: Маршрутизатор має різні моделі, але в основному вони мають 2 порти 10/100/1000 Ethernet (RJ-45) та 2 порти 10 Gigabit Ethernet (SFP+);

– модулі WAN: Маршрутизатор підтримує різні модулі WAN, такі як модуль портів ISDN, модуль портів T1/E1, модуль портів серії T3/E3 та інші;

– модулі серійного зв'язку: Маршрутизатор має слоти для розширення модулів серійного зв'язку, які підтримують різні інтерфейси, такі як асинхронний RS-232, RS-449, V.35 та інші;

– оперативна пам'ять: Варіюється залежно від конфігурації, але загалом має значний обсяг оперативної пам'яті для обробки даних та виконання завдань;

– жорсткий диск: Має вбудований жорсткий диск для зберігання конфігураційного програмного забезпечення та інших даних;

– підтримка мережевих протоколів: Включає підтримку IPv4, IPv6, BGP, OSPF, EIGRP, RIP та інших протоколів маршрутизації та комутації;

– безпека: Має різні механізми безпеки, такі як мережевий інспектор безпеки (Cisco IOS Firewall), IPSec VPN, SSL VPN, ACL (Access Control Lists) та інші;

– управління: Підтримує різні протоколи управління, включаючи SNMP (Simple Network Management Protocol), Telnet, SSH (Secure Shell), HTTPS та інші.

Комутатор Cisco Catalyst 2960X-24TS-L є частиною серії Catalyst 2960X, яка відома своєю надійністю та продуктивністю. Цей комутатор є популярним варіантом для невеликих і середніх мереж, офісних середовищ та інших сегментів ринку.

Основні характеристики комутатора Cisco Catalyst 2960X-24TS-L включають:

– комутатор має 24 порти 10/100/1000 Ethernet, що дозволяє підключати різноманітні пристрої, включаючи комп'ютери, принтери, IP-телефони та інші мережеві пристрої;

– він підтримує швидкість передачі даних на рівні 1 Gbps на кожен порт. Комутатор також має широкий пропускний здатність та підтримку різних протоколів для ефективного управління мережевим трафіком;

– catalyst 2960X-24TS-L надає різні функції управління, включаючи Cisco IOS Software, SNMP, RMON і т.д. Крім того, комутатор підтримує різні механізми безпеки, такі як IEEE 802.1X, ACL, Secure Shell (SSH), Secure Sockets Layer (SSL) та інші, для захисту мережевого трафіку та запобігання несанкціонованому доступу;

– він має вбудовані механізми для забезпечення високої доступності, включаючи функцію Hot Standby Redundancy Protocol (HSRP) та порти EtherChannel для створення забезпеченого з'єднання між комутаторами.

– catalyst 2960X-24TS-L підтримує технологію Energy Efficient Ethernet, яка автоматично регулює енергоспоживання в залежності від активності портів, зменшуючи споживання електроенергії та вплив на довкілля.

Повні технічні характеристики комутатора Cisco Catalyst 2960X-24TS-L:

– кількість портів: 24 порти Ethernet 10/100/1000 Mbps;
– підтримка PoE: Відсутня підтримка PoE (Power over Ethernet);
– стандарти Ethernet: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z;
– пропускна спроможність: До 48 Gbps;
– продуктивність протоколів мережі: До 35,7 млн. пакетів в секунду;
– буферна пам'ять: 2 МБ;
– VLAN: Підтримка до 4096 VLAN;
– розмір таблиці MAC-адрес: До 16 000 записів;
– QoS (Quality of Service): Підтримка QoS для пріоритизації даних та управління пропускною спроможністю;
– стандарти безпеки: Підтримка 802.1X, ACL (Access Control Lists), DHCP Snooping, IP Source Guard та інших механізмів безпеки;
– управління: Підтримка управління через консольний порт, Telnet, SSH (Secure Shell), SNMP (Simple Network Management Protocol) та інші протоколи управління;

– розмір: 1U (одиниця висоти);

– живлення: Підтримка внутрішнього блоку живлення.

Також для співробітників потрібні комп’ютери та монітори для роботи. Робочі машини співробітників офісу будуть представлені комп’ютерами ARTLINE BUSINESS B27 v34 та моніторами 27" Asus VA27EHE - 75 Hz

Характеристики робочих комп’ютерів:

– процесор: Intel Core i3-10100;

– кількість ядер: 4 ядра;

– частота центрального процесора: 3,6 - 4.3 GHz;

– об’ем ОЗУ: 8 ГБ;

– тип оперативної пам’яті: DDR4 2666 MHz;

– тип накопичувача: SSD, HDD;

– об’єм накопичувача: 240 GB, 2 TB;

– відеокарта: Intel UHD Graphics 630;

– мережеві інтерфейси: Адаптер LAN 10/100/1000 Kb/s.

Характеристики моніторів:

– діагональ екрану: 27";

– частота оновлення дисплею: 75 Гц;

– роздільна здатність: 192H0x1080 Full HD;

– час реакції матриці: 5 ms;

– тип матриці: IPS;

– інтерфейси: HDMI,VGA.

У якості серверів було обрано Asus Z11PA-D8. Він призначений для використання в центрах обробки даних для вирішення ресурсномістких обчислювальних завдань. Виробник надає можливість конфігурувати компоненти сервера, що дозоляє підібрати рішення, яке буде найбільш доцільним для потреб користувача.

Характеристики серверів:

- процесор: 2 x Десятиядерный Intel Xeon Silver 4114;

– кількість ядер: 10;

– частота центрального процесора: 2.2-3.0GHz;

– об’єм оперативної пам'яті: 128GB;

– тип оперативної пам’яті: DDR4-2666;

– тип накопичувача: HDD; - об’єм накопичувача: 12TB;

– мережеві інтерфейси: 4xGE RJ45.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування	Марка	Одиниця вимірювання	Кількість
1	Маршрутизатор ISR 4451-X	Cisco	шт.	6
2	Комутатор Catalyst 2960X-24TS-L	Cisco	шт.	10
3	Робочий комп’ютер Business b27 v34	Artline	шт.	75
4	Монітор для роботи VA27EHE	Asus	шт.	75
5	Сервер Z11PA-D8	Asus	шт.	4

2.4 Розрахунок інтенсивності трафіку найбільшої локальної мережі підприємства

Після детального огляду мережі, було виявлено локальну мереж з найбільшою кількістю вузлів, це відділ виробництва кондитерської фабрики “Житомирські Ласощі”.

Для розрахунку інтенсивності трафіку нам дано такі дані:

− кількість вузлів в найбільшій мережі: 250;

− середня інтенсивність трафіку: μ=94 (кадрів/с);

− середня довжина повідомлення: l=650 байт;

− вимоги до затримки передачі пакету – ≤ 6 мс;

− кількість портів комутатора − 24 шт.

Для початку потрібно розрахувати пропускну здатність мережі на рівні доступу, для цього використаємо формулу (2.1)

$$Pp.p = \mu * l * n, \quad (2.1)$$

де:

Pp.p – пропускна здатність мережі, біт/с;

μ – інтенсивність обслуговування, кадрів/с;

l – середня довжина повідомлення, байт;

n – кількість портів комутатора.

μ = 94 кадри/с;

l = 650 байт;

n = 24;

Pp.p = 94 * 650 * 24 = 11731200 ≈ 11.73 (Мбіт/с)

Далі потрібно розрахувати значення інтенсивності виходу, для цього використаємо формулу для розрахунку (2.2). Під час розрахунку, комутатор буде підключений через лінію 1000 Мбіт/с

$$\mu вих = C/ (8 * l), \quad (2.2)$$

де:

C – пропускна здатність лінії, біт/с;

l – середня довжина повідомлення байт.

C = 1 000 000 000 біт/с;

l = 650 байт.

μвих = 1 000 000 000 біт/с / (8 * 650) байт = 192 307 (пакетів/с)

Далі потрібно розрахувати максимальну кількість вузлів, що можна під’єднати до комутатора рівня розподілу, для цього використаємо формулу (2.3).

$$N = \mu вих / \mu, \quad (2.3)$$

де:

N – кількість вузлів, яку можна приєднати;

μвих – інтенсивність виходу, пакетів/с;

μ – середня інтенсивність трафіку, пакетів/с.

За отриманими даними з формули (2.3), інтенсивність виходу становить 192 307 пакетів/с, а середня інтенсивність трафіку дорівнює 94 пакетів/с.

Виходячи з цього отримуємо:

N = 192 307/ 94 ≈ 2045.8 (вузлів)

Згідно отриманих результатів, кількість вузлів що можна підключити до комутатора рівня розподілу вийшло 2045.8 = 2046. Результат був округлений до найближчого цілого значення.

Далі потрібно розрахувати загальну інтенсивність трафіку від усіх користувачів, для цього використаємо формулу (2.4).

$$\lambda = x * \mu, \quad (2.4)$$

де:

λ – загальна інтенсивність трафіку, пакети/с;

x – коефіцієнт, який представляє кількість користувачів або вузлів в мережі;

μ - середня інтенсивність трафіку, пакети/с.

x = 250;

μ = 94.

λ = 254*94 = 23500 (пакетів/с)

Далі потрібно розрахувати коефіцієнт затримки на рівні розподілу, для цього використаємо формулу (2.5)

$$\rho = \lambda / \mu_{вих}, \quad (2.5)$$

де:

ρ – коефіцієнт затримки на рівні розподілу;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу

λ = 23500 пакетів/с;

μвих = 192 307 пакетів/с.

ρ = 23500 / 192 307 ≈ 0.122

Далі потрібно розрахувати коефіцієнт зайнятості комутатора на рівні розподілу, використаємо формулу (2.6).

$$r = \rho / (1 - \rho), \quad (2.6)$$

де:

r – коефіцієнт зайнятості комутатора;

ρ – коефіцієнт затримки на рівні розподілу.

r = 0.122 / (1 - 0.122) = 0.138

Далі потрібно розрахувати середню затримку кадру, для цього використаємо формулу (2.7).

$$T = 1 / (\mu вих - \lambda), \quad (2.7)$$

де:

T – середня затримка кадру;

λ – загальна інтенсивність трафіку від всіх користувачів;

μвих – інтенсивність виходу

λ = 23500 пакетів/с;

μвих = 192 307 пакетів/с.

$T = 1 / (192\ 307 – 23500) = 59 * 10^{-6}$(секунд)

Далі потрібно розрахувати середню довжину черги, для цього використаємо формулу (2.8).

$$Lчерги = \rho^2 / (1 - \rho), \quad (2.8)$$

де:

Lчерги – середня довжина черги;

ρ – коефіцієнт затримки на рівні розподілу.

Lчерги = $(0.122)^2$ / (1 - 0.122) = 0.016

Після розрахунку середньої довжини черги, потрібно розрахувати середній час пакету у черзі, для цього використовуємо формулу (2.9).

$$Точік = Lчерги / \lambda, \quad (2.8)$$

де:

Точік – середній час перебування пакета в черзі;

Lчерги – середня довжина черги;

λ – загальна інтенсивність трафіку від всіх користувачів.

Точік = 0.016 / 23500 = 0.680 (мс)

Для потрібно розрахувати пропускну здатность каналу, для цього використаємо формулу (2.9).

$$b = \lambda * l*8, \quad (2.9)$$

де:

b - пропускна здатність каналу, біт/с;

λ - інтенсивність трафіку, пакетів/с;

l - середня довжина пакету, байт.

λ = 23500 пакетів/с;

l = 650 байт.

b = (23500 * 650*8) / 10^{-6} = 122 Мбіт/с.

Отриманий результат задовольняє вихідний канал 1000 Мбіт/с.

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА НАЛАШТУВАННЯ КОМП'ЮТЕНОЇ СИСТЕМИ

3.1 Розрахунок схеми адресації корпоративної мережі

Для того що побудувати мережу кондитерської фабрики "Житомирські Ласощі" був використаний адресний простір 172.23.72.0/21. У даному випадку, маска підмережі /21 використовує 21 біт для мережі і залишає 11 біт для хостів.

Отже, в даній мережі можливо підключити до 2^11 (або 2048) хостів. Для того щоб розрахувати підмережі буде використовуватися метод VLSM.

VLSM (Variable Length Subnet Masking) є методом розподілу IP-адрес та масок підмереж, який дозволяє ефективно використовувати доступні адреси та мінімізувати втрати IP-адрес при створенні підмереж.

Основна ідея VLSM полягає в тому, що різні підмережі можуть мати різні розміри в залежності від вимог мережі. Таким чином, можна розподілити IP-адреси більш точно, а не прив'язуватися до стандартних масок підмереж, які мають фіксований розмір.

Переваги використання VLSM включають:

– ефективне використання адрес: Метод VLSM дозволяє використовувати різні маски підмереж для різних частин мережі, що дозволяє економити IP-адреси і забезпечувати оптимальне використання наявних ресурсівl;

– гнучкість: Завдяки VLSM можна створювати підмережі різного розміру залежно від конкретних потреб мережі. Це дозволяє забезпечувати достатню кількість IP-адрес для більших підмереж і меншу кількість для менших під мереж;

– скорочення втрат IP-адрес: Використовуючи VLSM, можна уникнути зайвих втрат IP-адрес, оскільки адреси можна розподілити більш точно і не виділяти великі блоки IP-адрес для малих підмереж.

Для розрахунку мережі за допомогою VLSM, потрібно визначити кількість хостів у кожній підмережі та вибрати маски підмереж, які забезпечать потрібну кількість адрес. За допомогою VLSM можна ефективно використовувати IP-адреси, зменшити кількість втрат та забезпечити гнучкі

Для прикладу розрахунку візьмемо підмережу «Відділ виробництва» яка має 250 вузлів, вона є найбільшою підмережею, для неї також розраховувалась інтенсивність трафіку.

Спочатку почнемо з розрахунку потрібної маски підмережі, спочатку знайдемо найменшу степінь двійки, яка перевищує 250. У цьому випадку, найближча степінь двійки, що більша за 250, це 256 (2^8).

Маска підмережі для 256 адрес може бути /24 (32 - 21 = 11 біт для хостів). Отже, нам потрібно 8 бітів для хостів.

Тепер після розрахунку VLSM методом мережева адреса буде 172.23.72.0, діапазон адреса 172.23.72.1 - 172.23.72.254, широкомовна адреса 172.23.72.255, а маска під мережі /24.

Це був приклад для розрахунку підмереж методом VLSM , всі інші підмережі будут розраховуватися по аналогії.

В таблиці 3.1 зображена схема адресації корпоративної мережі кондитерської фабрики “Житомирські ласощі“. Всі розрахунки були за методом VLSM.

Таблиця 3.1 – Схема адресації корпоративної мережі кондитерської фабрики “Житомирські ласощі“

Назва підмережі	Кількість вузлів	Номер мережі	Маска мережі	Діапазон
Відділ виробництва	250	172.23.72.0	255.255.255.0/24	172.23.72.1 – 172.23.72.254
Відділ керівництва	38	172.23.75.0	255.255.255.192/26	172.23.75.1 – 172.23.75.62

Продовження таблиці 3.1

Віддалена мережа	100	172.23.73.0	255.255.255.128/25	172.23.73.1 – 172.23.73.126
Відділ технічної підтримки	61	172.23.74.0	255.255.255.192/26	172.23.74.1 - 172.23.74.62
Відділ маркетингу та збуду	39	172.23.74.192	255.255.255.192/26	172.23.74.193 – 172.23.74.254
Відділ якості і продукції	50	172.23.74.128	255.255.255.192/26	172.23.74.129 – 172.23.74.190
Відділ кадрів та управління персоналом	67	172.23.73.128	255.255.255.128/25	172.23.73.129 – 172.23.73.254
Відділ закупівель та логістики	55	172.23.74.64	255.255.255.192/26	172.23.74.65 – 172.3.74.126
Охорона	35	172.23.75.64	255.255.255.192/26	172.23.75.65 – 172.23.75.125
WAN1	2	10.0.4.0	255.255.255.252/30	10.0.4.1 – 10.0.4.2
WAN2	2	10.0.4.4	255.255.255.252/30	10.0.4.5 – 10.0.4.6
WAN3	2	10.0.4.8	255.255.255.252/30	10.0.4.9 – 10.0.4.10
WAN4	2	10.0.4.12	255.255.255.252/30	10.0.4.13 – 10.0.4.14
WAN5	2	10.0.4.16	255.255.255.252/30	10.0.4.17 – 10.0.4.18
WAN6	2	10.0.4.20	255.255.255.252/30	10.0.4.21 – 10.0.4.22
WAN7	2	64.100.13.0	255.255.255.252/30	64.100.13.1 64.100.13.2
WAN_IPS	2	209.165.202.0	255.255.255.252/30	209.165.202.1 – 209.165.202.2
VLAN14	27	172.23.72.0	255.255.255.224/27	172.23.72.1 – 172.23.72.30

Продовження таблиці 3.1

VLAN24	27	172.23.72.32	255.255.255.224/27	172.23.72.33 – 172.23.72.62
VLAN34	27	172.23.72.64	255.255.255.224/27	172.23.72.65 – 172.23.72.94
VLAN44	27	172.23.72.96	255.255.255.224/27	172.23.72.97 – 172.23.72.126
VLAN54	27	172.23.72.128	255.255.255.224/27	172.23.72.129 – 172.23.72.158
VLAN64	27	172.23.72.160	255.255.255.224/27	172.23.72.161 – 172.23.72.190
VLAN74	27	172.23.72.192	255.255.255.224/27	172.23.72.193 – 172.23.72.222
VLAN84	6	172.23.72.240	255.255.255.248/29	172.23.72.241 – 172.23.72.246
VLAN99	10	172.23.72.224	255.255.255.240/28	172.23.72.225 – 172.23.72.238

3.2 Розрахунок схеми адресації пристроїв

Для того щоб скласти таблицю адресації пристроїв кондитерської фабрики “Житомирські Ласощі”, треба використовувати такі технічні вимоги:

1. Перший набір IP-адрес призначений інтерфейсам і підінтерфейсам маршрутизаторів у локальній мережі.
2. Другий набір IP-адрес призначається комутаторам у кожній локальній мережі.
3. Сервери налаштовані з IP-адресами, які обчислюються за правилом: IPадрес = перший можливий адрес у мережі + 9 + 4.
4. Останні доступні IP-адреси призначені вузлам.
5. В під мережах VLAN використовується протокол DHCP для автоматичного призначення IP-адрес кінцевим пристроям.

На основі технічних вимог та розрахованих даних які були наведені у таблиці 3.1, була складена схема адресації пристроїв, яка представлена у таблиці 3.2.

Таблиця 3.2 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Grechen_Router_0	Gig0/0/0	64.100.13.2	/30	–	–	Gig0/0/1
	Gig0/0/1	172.23.73.1	/25	–	–	Gig0/1
Grechen_Router _1	Se0/1/0	10.0.4.18	/30	–	–	Se0/1/0
	Se0/1/1	10.0.4.14	/30	–	–	Se0/1/1
	Gig0/0/1	172.23.73.129	/25	–	–	Gig0/1
	Gig0/0/0	172.23.74.1	/26	–	–	Gig0/1
Grechen_Router_2	Gig0/0/1	10.0.4.6	/30	–	–	Gig0/0/0
	Gig0/0/2	10.0.4.10	/30	–	–	Gig0/0/1
	Gig0/0/0	10.0.4.1	/30	–	–	Gig0/0/2
Grechen_Router_3	Se0/1/0	209.165.202.2	/30	–	–	Se0/1/0
	Gig0/0/1	172.23.74.65	/26	–	–	Gig0/1
	Gig0/0/0	172.23.74.193	/26	–	–	Gig0/1
	Gig0/0/2	172.23.74.129	/26	–	–	Gig0/1
	Se0/1/1	10.0.4.21	/30	–	–	Se0/2/0
Grechen_Router_4	Gig0/0/2	172.23.75.1	/26	–	–	Gig0/1
	Se0/1/0	10.0.4.17	/30	–	–	Se0/1/0
	Se0/1/1	10.0.4.13	/30	–	–	Se0/1/1
	Se0/2/0	10.0.4.22	/30	–	–	Se0/1/1
	Gig0/0/0	10.0.4.5	/30	–	–	Gig0/0/1
	Gig0/0/1	10.0.4.9	/30	–	–	Gig0/0/2
Grechen_Router_5	Gig0/0/2	10.0.4.2	/30	–	–	Gig0/0/0
	Gig0/0/1	172.23.75.65	/26	–	–	Gig0/1
	Gig0/0/0	172.23.72.1	/24	–	–	Gig0/1
Grechen_IPS	Se0/1/0	209.165.202.1	/30	–	–	Se0/1/0
	Gig0/0/1	64.100.13.1	/30	–	–	Gig0/0/0

Продовження таблиці 3.2

	Gig0/0/0	209.165.201.5	/30	–	–	NIC
Grechen_Switch_0	VLAN1	172.23.73.2	/25	172.23.73.1	–	PC_3.1 – PC_3.2 Server TFTP NIC
Grechen_Switch_1.1	VLAN1	172.23.72.2	/24	172.23.72.1	–	Fa0/1 – Fa0/9
Grechen_Switch_1.2	VLAN1	172.23.72.3	/24	172.23.72.1	–	PC_1.1 Server IoT
Grechen_Switch_3	VLAN1	172.23.74.2	/26	172.23.74.1	–	PC_4.1 – PC_4.10 NIC
Grechen_Switch_4	VLAN1	172.23.73.130	/25	172.23.73.129	–	PC_7.1 – PC_7.9 NIC
Grechen_Switch_5	VLAN1	172.23.74.194	/26	172.23.74.193	–	PC_5.1 – PC_ 5.11 Server DNS NIC
Grechen_Switch_6	VLAN1	172.23.74.66	/26	172.23.74.65	–	PC_6.1 – PC_6.12 NIC
Grechen_Switch_7	VLAN1	172.23.74.130	/26	172.23.74.129	–	PC_6.1 – PC_1.12 NIC
Grechen_Switch_8	VLAN1	172.23.75.2	/26	172.23.75.1	–	PC_2.1 – PC_2.3 Server HTTP NIC
Grechen_Switch_9	VLAN1	172.23.75.66	/26	172.23.75.65	–	PC_9.1 – PC_9.4 NIC
Server HTTP	NIC	172.23.75.14	/26	172.23.75.1		Gig0/2
Server DNS	NIC	172.23.74.206	/26	172.23.74.193		Gig0/2
Server TFTP	NIC	172.23.73.14	/25	172.23.73.1		Gig0/2
Server IoT	NIC	172.23.72.14	/24	172.23.72.1		Gig0/2

3.3 Розробка топологічної схеми підприємства

Згідно технічних вимог та таблиць адресації 3.1-3.2 була розроблена топологічна схема кондитерської фабрики “Житомирські Ласощі”.

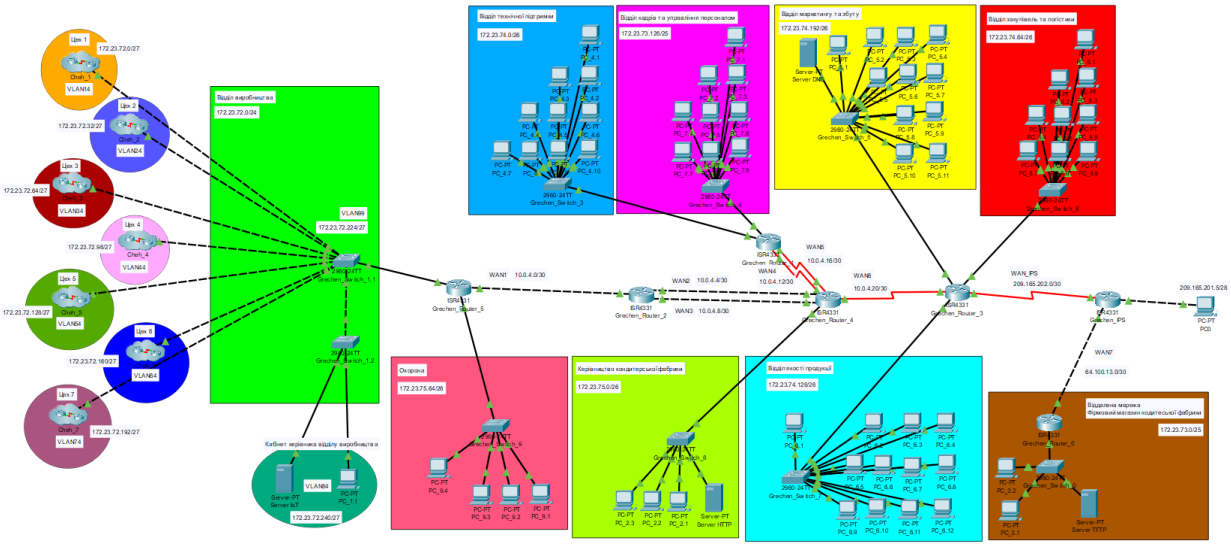

Рисунок 3.1 – Топологічна схема кондитерської фабрики “Житомирські Ласощі”

3.4 Базове налаштування конфігурації пристроїв

Згідно технічних вимог потрібно виконати базове налаштування пристроїв:

– надано унікальні ім’я пристроям;

– налаштовано пароль cisco на консолі та лінії vty;

– застосовано пароль class для привілейованого режиму;

– забезпечено шифрування усіх паролів;

– виконано налаштування банеру MOTD;

– налаштовано на лініях vty застосування протоколу ssh;

– назначено користувача 12320sk1_Grechen з паролем admincisco;

– використовуючи ім’я пристрою налаштовано ім’я домену та згенеровано ключ RSA завдовжки 1024 біт;

– встановлено значення тактової частоти 128000 на DCE-інтерфейсах маршрутизаторів;

− з використанням локальної бази було налаштовано аудит і відправку повідомлень про початок і завершення процесу exec.

Приклади налаштування пристроїв згідно технічних умов для комп'ютерної системи кондитерської фабрики "Житомирські Ласощі":

Для того щоб надати пристрою унікального ім'я, треба використати команду *hostname:*

Router(config)#hostname Grechen_Router_5

Далі потрібно налаштувати паролі, згідно технічних умов, треба використовувати пароль "cisco" на консолі та лінії vty 0 15:

Grechen_Router_5(config)#line console 0

Grechen_Router_5(config-line)#password cisco

Grechen_Router_5(config-line)#login

Grechen_Router_5(config-line)#exit

Grechen_Router_5(config)#line vty 0 15

Grechen_Router_5(config-line)#password cisco

Grechen_Router_5(config-line)#login

Grechen_Router_5(config-line)#exit

Далі потрібно налаштувати пароль для входу у привілейований режим, згідно технічних умов, треба використовувати пароль "class":

Grechen_Router_5(config)#enable secret class

Далі згідно технічних умов треба використати сервіс шифрування усіх паролів, які у відкритому доступі:

Grechen_Router_5(config)#service password-encryption

Далі згідно технічних умов треба налаштувати банер MOTD:

Grechen_Router_5 (config)#banner motd #Grechen_Router_5. You enter in sekure area#

Далі згідно технічних умов треба налаштувати протокол SSH:

– створення домену:

Grechen_Router_5(config)#ip domain name Grechen_Router_5

– генерація ключа RSA довжиною 1024 bit:

Grechen_Router_5(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

– налаштування версії протоколу SSH:

Grechen_Router_5(config)#ip ssh version 2

– створення користувача 12320sk1_Grechen з паролем admincisco:

Grechen_Router_5(config)#username 12320sk1_Grechen privilege 15 password admincisco

– налаштування протоколу SSH лініях VTY 0 15:

Grechen_Router_5(config)#line vty 0 15

Grechen_Router_5(config-line)#transport input ssh

Grechen_Router_5(config-line)#login local

Grechen_Router_5(config-line)#exec-time 60 0

Далі згідно технічних вимог встановити IP-адрес на інтерфейсах, відповідно до таблиці 3.2:

Grechen_Router_5(config)#int g0/0

Grechen_Router_5(config-if)#ip address 172.23.72.1 255.255.255.0

Grechen_Router_5(config-if)#no shut down

Grechen_Router_5(config-if)#exit

На DCE-інтерфейсах налаштування тактової частоти 128000:

Grechen_Router_3(config-if)#clock rate 128000

Інші базові налаштування для пристроїв будуть по аналогії як в прикладі

3.5 Налаштування маршрутизаторів

Згідно технічних вимог для організації динамічної маршрутизації у комп’ютерній системі кондитерської фабрики “Житомирські Ласощі” використовується протокол OSPF

Переваги протоколу OSPF:

– масштабованість: OSPF дозволяє ефективно працювати в великих мережах, підтримуючи тисячі маршрутизаторів та під мереж;

– швидка збіжність: OSPF забезпечує швидку збіжність мережі, що означає, що маршрутизатори швидко визначають найкращі маршрути та оновлюють таблиці маршрутизації при зміні топології мережі;

– підтримка різних метрик: OSPF дозволяє задавати різні метрики для визначення найкращих шляхів маршрутизації, таких як пропускна здатність та затримка, що дозволяє більш гнучко керувати трафіком в мережі;

– підтримка IPv6: OSPFv3 є повністю сумісним з IPv6, що важливо для майбутнього розвитку мереж.

Для прикладу налаштування маршрутизації будуть наведені на Grechen_Router_3:

– активація протоколу маршрутизації OSPF з вказанням номеру процесу OSPF, який буде використовуватися:

Grechen_Router_3(config)#router ospf 4

– призначення маршрутизаторові власного id:

Grechen_Router_3(config)#router-id 3.3.3.3

– додавання мереж до області маршрутизації 0:

Grechen_Router_3(config-router)#network 172.23.74.192 0.0.0.63 area 0

Grechen_Router_3(config-router)#network 10.0.4.20 0.0.0.3 area 0

Grechen_Router_3(config-router)#network 172.23.74.64 0.0.0.63 area 0

Grechen_Router_3(config-router)#network 172.23.74.128 0.0.0.63 area 0

Далі згідно технічних вимог потрібно налаштувати статичний маршрут на маршрутизаторі, який має пряме підключення до маршрутизатора провайдера:

Grechen_Router_3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1

Згідно технічних вимог до розробки на serial-інтерфейсах виконується налаштування пропускної спроможності та значення метрики OSPF:

– перехід до налаштування інтерфейсу Serial 0/0/1:

Grechen_Router_3(config)#int se0/1/1

– встановлення значення пропускної здатності 128Кбіт/с:

Grechen_Router_3(config-if)#bandwidth 128

– встановлення значення метрики на 7500:

Grechen_Router_3(config-if)#ip ospf cost 7500

Інші маршрутизатори будуть налаштовані по аналогії як в прикладі.

3.6 Налаштування маршрутизаторів на підтримку служби AAA

Служба AAA (Authentication, Authorization, and Accounting) є ключовою складовою сучасних комп'ютерних мереж та систем управління доступом. Вона забезпечує механізми для аутентифікації користувачів, надання прав доступу та обліку їх дій в мережі.

Основні компоненти служби AAA включають:

– аутентифікація (Authentication): Аутентифікація перевіряє ідентичність користувача, що намагається отримати доступ до ресурсів мережі. Це може бути досягнуто за допомогою різних методів, таких як введення логіна та пароля, використання сертифікатів, біометричних даних тощо;

– авторизація (Authorization): Після успішної аутентифікації служба AAA надає механізми для визначення дозволів та обмежень доступу користувача. Це означає, що система визначає, які ресурси та операції може виконувати користувач після успішного входу в систему;

– облік (Accounting): Служба AAA веде облік дій користувачів, який може включати інформацію про час входу/виходу, обсяг переданих даних, виконані операції тощо. Це дозволяє відстежувати активність користувачів, забезпечувати безпеку мережі та здійснювати аудит системи.

Застосування служби AAA дозволяє підвищити безпеку мережі, контролювати доступ користувачів до ресурсів та проводити аналіз активності в мережі.

Для прикладу налаштування служби AAA будуть наведены на маршрутизаторі Grechen_Router_5:

Grechen_Router_5(config)#aaa new-model

Grechen_Router_5(config)#aaa authentication login default group radius local

Налаштування RADIUS-сервера:

Grechen_Router_5(config)#radius server MyRadiusServer

Grechen_Router_5(config-radius-server)#addr ipv4 172.23.74.206

Grechen_Router_5(config-radius-server)#key radius123

Grechen_Router_5(config-radius-server)#exit

Налаштування аутентифікації для консольної лінії та VTY:

Grechen_Router_5(config)#line console 0

Grechen_Router_5(config-line)#login authentication default

Grechen_Router_5(config-line)#line vty 0 15

Grechen_Router_5(config-line)#login authentication default

На рисунку 3.2 зображено успішний вхід до маршрутизатора Grechen_Router_5 через аутентифікацію сервера RADIUS

Інші маршрутизатори будуть налаштовані по аналогії як в прикладі.

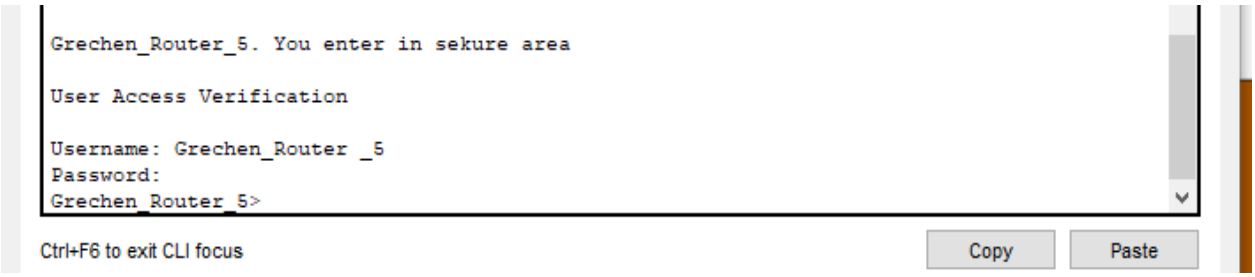

Рисунок 3.2 – Аутентифікація через RADIUS сервер

3.7 Налаштування роботи інтернет

Згідно технічних вимог для того організувати доступ робочих станцій підприємства до Інтернету, на прикордонному маршрутизаторі потрібно застосувати технологію NAT.

NAT (Network Address Translation) - це процес перетворення IP-адрес мережевого пристрою на інший IP-адрес. Це використовується для

забезпечення зв'язку між пристроями в різних локальних мережах або мережі Інтернет.

Головна функція NAT полягає в перетворенні приватних IP-адрес на глобальні (зовнішні) IP-адреси і навпаки. Приватні IP-адреси використовуються в локальних мережах для ідентифікації пристроїв, а глобальні IP-адреси використовуються в Інтернеті для забезпечення комунікації між мережами.

При використанні NAT, мережевий пристрій, такий як маршрутизатор або брандмауер, виконує перетворення IP-адрес, коли пакети проходять через нього. Коли пристрій з внутрішньою приватною IP-адресою намагається вийти в Інтернет, NAT замінює його IP-адресу на глобальну IP-адресу, яка призначена пристрою маршрутизатора. При отриманні відповіді від зовнішнього сервера NAT перетворює глобальну IP-адресу назад на приватну IP-адресу і направляє пакети до відповідного пристрою в локальній мережі.

На пограничному маршрутизаторі Grechen_Router_3 було налаштовано NAT відповідно до технічних вимог, що включають наступні параметри:

– ім'я пулу Internet;

– пул IP-адрес від 209.165.202.5 до 209.165.202.30;

– адреса серверу HTTP 209.165.200.4;

– номер списку доступу 4.

Налаштування NAT на маршрутизаторі Grechen_Router_3:

– створення списку доступу з номером 4, який дозволяє трафіку з мережі 172.23.72.0/21 проходити через NAT:

Grechen_Router_3(config)#access-list 4 permit 172.23.72.0 0.0.7.255

– створення пулу IP-адрес з назвою "Internet" від 209.165.202.5 до 209.165.202.30 з маскою підмережі 255.255.255.224. Цей пул буде використовуватися для перетворення приватних адрес в публічні:

Grechen_Router_3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

– налаштування використання пулу "Internet" для перетворення IP-адрес, що відповідають списку доступу 4:

Grechen_Router_3(config)*#ip nat inside source list 4 pool Internet*

– задання статичного NAT, де локальна IP-адреса 172.23.75.14 буде перетворена на публічну IP-адресу 209.165.202.4:

Grechen_Router_3(config)#ip nat inside source static 172.23.75.14 209.165.202.4

– налаштування інтерфейсу маршрутизатора, як зовнішній інтерфейс для NAT. Цей інтерфейс з'єднується з Інтернетом:

Grechen_Router_3(config)#int se0/1/0

Grechen_Router_3(config-if)#ip nat outside

– встановлення інтерфейсу se0/1/1, як внутрішнього інтерфейсу для NAT:

Grechen_Router_3(config-subif)#in se0/1/1

Grechen_Router_3(config-if)#ip nat inside

На рисунку 3.3 зображено таблицю перетворень NAT на маршрутизаторі Grechen_Router_3.

NAT Table for Grechen_Router_3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.5:16	172.23.72.14:16	172.23.73.14:16	172.23.73.14:16
icmp	209.165.202.5:19	172.23.72.14:19	172.23.73.14:19	172.23.73.14:19
icmp	209.165.202.4:13	172.23.75.14:13	172.23.73.14:13	172.23.73.14:13
icmp	209.165.202.4:7	172.23.75.14:7	172.23.73.14:7	172.23.73.14:7

Рисунок 3.3 – Таблиця перетворень NAT на Grechen_Router_3

3.8 Налаштування VPN

VPN site-to-site – це тип віртуальної приватної мережі, яка забезпечує безпечний обмін даними між двома або більше віддаленими локальними мережами чи мережними пристроями через публічну мережу, таку як Інтернет. Цей тип VPN є часто використовуваним рішенням для забезпечення зв'язку між розподіленими офісами, філіями компаній, віддаленими центрами обробки даних та іншими мережами.

У VPN site-to-site кожна локальна мережа або мережний пристрій має власний VPN-шлюз, який виконує функції шифрування та декодування даних, а також передачі даних через публічну мережу. VPN-шлюзи встановлюють VPN-тунель між собою, що дозволяє передавати дані в зашифрованому вигляді.

При використанні VPN site-to-site всі дані, які передаються між віддаленими мережами або пристроями, захищені за допомогою шифрування. Це забезпечує конфіденційність та безпеку даних, що передаються через незахищену публічну мережу, таку як Інтернет.

Для прикладу налаштувань VPN будуть наведі на маршрутизаторі Grechen_Router_3:

Для початку потрібно налаштувати списки контролю доступу:

Grechen_Router_3(config)ip access-list extended 104

Grechen_Router_3(config-ext-nacl)#permit ip any 209.165.200.0 0.0.0.3

Grechen_Router_3(config-ext-nacl)#permit ospf any any

Grechen_Router_3(config)#ip access-list extended VPN

Grechen_Router_3(config-ext-nacl)#permit ip 172.23.72.0 0.0.7.255 172.23.73.0 0.0.0.127

Далі здійснюється налаштування ISAKMP політики та ключа, що встановлює специфічні параметри шифрування та аутентифікації, які будуть використовуватися.

Grechen_Router_3(config)#crypto isakmp policy 1

Grechen_Router_3(config-isakmp)#encryption aes 256

Grechen_Router_3(config-isakmp)#authentication pre-share

Grechen_Router_3(config-isakmp)#group 1

Grechen_Router_3(config)#crypto isakmp key cisco address 64.100.13.2

Далі налаштовується трансформація IPsec яка визначає конкретні методи шифрування та хешування, що будуть використовуватися під час установки IPsec-з'єднання.

Grechen_Router_3(config)#crypto ipsec transform-set VPN-IPSEC-SET esp-aes esp-sha-hmac

Далі виконується створення криптографічного мапування під назвою VPN-MAP з ідентифікатором 4 і вказування протоколів IPsec і ISAKMP:

Grechen_Router_3(config)#crypto map VPN-MAP 4 ipsec-isakmp

Далі Встановлюється IP-адреса віддаленого піра (VPN-концентратора) як 64.100.13.2:

Grechen_Router_3(config-crypto-map)#set peer 64.100.13.2

Далі вказується набору трансформацій VPN-IPSEC-SET для шифрування і хешування пакетів IPsec:

Grechen_Router_3(config-crypto-map)#set transform-set VPN-IPSEC-SET

Далі встановлюються відповідності (match) зовнішнього списку доступу (ACL) з назвою FOR-VPN для визначення трафіку, який буде захищений IPsec:

Grechen_Router_3(config-crypto-map)#match address FOR-VPN

Grechen_Router_3(config-crypto-map)#exit

Після цього налаштувується криптографічне мапування VPN-MAP на інтерфейсі Serial 0/1/0:

Grechen_Router_3 (config)#interface Serial 0/1/0

Grechen_Router_3(config-if)#crypto map VPN-MAP

, На рисунку 3.4 та 3.5 зображено результати виконання двух команд *Grechen_Router_3#show crypto ipsec sa* та *Grechen_Router_3#show crypto isakmp sa*

```
Grechen_Router_3#sh crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 209.165.202.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.23.72.0/255.255.248.0/0/0)
   remote  ident (addr/mask/prot/port): (172.23.73.0/255.255.255.128/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.202.2, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x940CB693(2483861139)
```

Рисунок 3.4 – Перевірка стану IPSec SA на Grechen_Router_3

```
Grechen_Router_3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
64.100.13.2     209.165.202.2   QM_IDLE           1046    0 ACTIVE
```

Рисунок 3.5 – Вивід усіх існуючих ISAKMP SA на Grechen_Router_3

3.9 Розробка методів для захисту інформації в комп'ютерній системі

3.9.1 Налаштування мереж VLAN

Для спрощення керування в цехах виробничого відділу потрібно розділити на логічні окремі сегменти. Кожен цех будет окремим VLAN.

Використання VLAN приводить до економії на додатковому обладнанні та зниження витрат на впровадження та обслуговування мережі. Окрім вигод у сфері економіки, використання VLAN також забезпечує покращення безпеки мережі шляхом логічного відокремлення різних груп користувачів.

Використовуючи VLAN, у майбутньому можна масштабувати мережу за потреби. Також можена додавати або видаляти VLAN, а також змінювати їх конфігурацію, не зачіпаючи іншу мережу. Це особливо корисно у разі розширення організації або змін в структурі цехів і відділів.

В таблиці 3.3 представлено розподілення підмережі «Відділ продажу» на VLAN.

Таблиця 3.3 – Список мереж VLAN

Номер VLAN	Назва VLAN	Примітка
1	default	Не використовується
14	Cheh_1	Цех 1
24	Cheh_2	Цех 2
34	Cheh_3	Цех 3
44	Cheh_4	Цех 4
54	Cheh_5	Цех 5
64	Cheh_6	Цех 6
74	Cheh_7	Цех 7
84	Office_of_the_head_of_ the_production_department	Кабінет керівника відділу виробництва
99	Management	Для управління пристроями
100	Native	Власна мережа

Для прикладу налаштування VLAN використовувався комутатор Grechen_Switch_1.1*:*

Grechen_Switch_1.1(config)#int g0/1

Grechen_Switch_1.1(config-if)#switchport mode trunk

Grechen_Switch_1.1(config-if)#switchport trunk native vlan 100

Grechen_Switch_1.1(config-if)#switchport trunk allowed vlan 14,24,34,44, 54,64,74,84,99-100

Далі потрібно створити VLAN 14, 24, 34, 44, 54, 64, 74, 84, 99, 100 і надати їм належне найменування:

Grechen_Switch_1.1(config)#vlan 14

Grechen_Switch_1.1(config-vlan)#name Cheh_1

Grechen_Switch_1.1(config-vlan)#vlan 24

Grechen_Switch_1.1(config-vlan)#name Cheh_2

Grechen_Switch_1.1(config-vlan)#vlan 34

Grechen_Switch_1.1(config-vlan)#name Cheh_3

Grechen_Switch_1.1(config-vlan)#vlan 44

Grechen_Switch_1.1(config-vlan)#name Cheh_4

Grechen_Switch_1.1(config-vlan)#vlan 54

Grechen_Switch_1.1(config-vlan)#name Cheh_5

Grechen_Switch_1.1(config-vlan)#vlan 64

Grechen_Switch_1.1(config-vlan)#name Cheh_6

Grechen_Switch_1.1(config-vlan)#vlan 74

Grechen_Switch_1.1(config-vlan)#name Cheh_7

Grechen_Switch_1.1(config-vlan)#vlan 84

Grechen_Switch_1.1(config-vlan)#name Office_of_the_head _of_the_production_department

Grechen_Switch_1.1(config-vlan)#vlan 99

Grechen_Switch_1.1(config-vlan)#name Management

Grechen_Switch_1.1(config-vlan)#vlan 100

Grechen_Switch_1.1(config-vlan)#name Native

Далі потрібно налаштувати VLAN 99 на прикладі Grechen_Switch_1.1:

Grechen_Switch_1.1(config)#int vlan 99

Grechen_Switch_1.1(config-if)#description LAN vlan_99_Sw_1.1

Grechen_Switch_1.1(config-if)#ip add 172.23.72.226 255.255.255.240

Grechen_Switch_1.1(config-if)#no shutdown

Grechen_Switch_1.1(config-if)#ip default-gateway 172.23.72.225

Далі виконується створення саб інтерфейсів, кожен з яких використовує протокол 802.1Q (dot1Q), налаштування відбуваються на прикладі Grechen_Router_5:

Grechen_Router_5(config)#int g0/0/0

Grechen_Router_5(config-if)#no sh

Grechen_Router_5(config-if)#int g0/0/0.14

Grechen_Router_5(config-subif)#encapsulation dot1Q 14

Grechen_Router_5(config-subif)#ip addr 172.23.72.1 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5(config-subif)#int g0/0/0.24

Grechen_Router_5(config-subif)#encapsulation dot1Q 24

Grechen_Router_5(config-subif)#ip addr 172.23.72.33 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.34

Grechen_Router_5(config-subif)#encapsulation dot1Q 34

Grechen_Router_5(config-subif)#ip addr 172.23.72.65 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.44

Grechen_Router_5(config-subif)#encapsulation dot1Q 44

Grechen_Router_5(config-subif)#ip addr 172.23.72.97 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.54

Grechen_Router_5(config-subif)#encapsulation dot1Q 54

Grechen_Router_5(config-subif)#ip addr 172.23.72.129 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.64

Grechen_Router_5(config-subif)#encapsulation dot1Q 64

Grechen_Router_5(config-subif)#ip addr 172.23.72.161 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.74

Grechen_Router_5(config-subif)#encapsulation dot1Q 74

Grechen_Router_5(config-subif)#ip addr 172.23.72.193 255.255.255.224

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5 (config-subif)#int g0/0/0.84

Grechen_Router_5(config-subif)#encapsulation dot1Q 84

Grechen_Router_5(config-subif)#ip addr 172.23.72.241 255.255.255.248

Grechen_Router_5(config-subif)#no sh

Grechen_Router_5(config-subif)#int g0/0/0.99

Grechen_Router_5(config-subif)#encapsulation dot1Q 99

Grechen_Router_5(config-subif)#ip addr 172.23.72.225 255.255.255.240

Grechen_Router_5(config-subif)#no sh

Далі потрібно налаштувати діапазони інтерфейсів для кожного VLAN на прикладі Grechen_Switch_7.1.1

Grechen_Switch_7.1.1(config)#int range Fa0/1-12

Grechen_Switch_7.1.1(config-if-range)#switchport mode access

Grechen_Switch_7.1.1(config-if-range)#switchport access vlan 74

Grechen_Switch_7.1.1(config-if-range)#exit

Grechen_Switch_7.1.1(config)# int range Fa0/14-24

Grechen_Switch_7.1.1(config-if-range)#switchport mode access

Grechen_Switch_7.1.1(config-if-range)#switchport access vlan 74

Grechen_Switch_7.1.1(config-if-range)#exit

Згідно технічних вимог для користувачів у віртуальних мережах VLAN, налаштування будуть отримуватися за протоколом DHCP, приклад налаштувань на Grechen_Router_5 для VLAN64:

Grechen_Router_5(config)#ip dhcp pool Vlan64pool

Grechen_Router_5(dhcp-config)#network 172.23.72.160 255.255.255.224

Grechen_Router_5(dhcp-config)#default-router 172.23.72.161

Grechen_Router_5(dhcp-config)#dns-server 172.23.74.206

Інші пристрої будуть для організації VLAN будуть налаштовані по аналогії наведених прикладів.

3.9.2 Налаштування безпеки портів на комутаторах

Згідно технічних вимог на портах комутаторів підключених до серверів, потрібно налаштувати функцію безпеки портів

Безпека портів комутатора відіграє важливу роль у забезпеченні безпеки мережі. Ось декілька причин, чому безпека портів комутатора є важливою:

– попередження несанкціонованого доступу: Безпека портів комутатора дозволяє обмежити фізичний доступ до мережі. Відключення не використовуваних портів або використання механізмів аутентифікації, таких як 802.1X, допомагає запобігти несанкціонованому доступу до мережі;

– захист від внутрішніх атак: Компрометація одного пристрою всередині мережі може становити загрозу для інших пристроїв. Безпека портів комутатора дозволяє налаштувати політики безпеки для обмеження комунікації між портами або сегментами мережі, запобігаючи поширенню внутрішніх атак у мережі.

Для прикладу функцію безпеки портів було продемонстровано на комутаторі Grechen_Switch_1.2, до порта G0/2 підключен IoT сервер, приклад:

Grechen_Switch_1.2(config)#int G0/2

Grechen_Switch_1.2(config-if)#switchport port-security maximum 2

Grechen_Switch_1.2(config-if)#switchport port-security mac-address sticky

Grechen_Switch_1.2(config-if)#switchport port-security violation shutdown

Інші пристрої були налаштовані по аналогії цього прикладу.

3.10 Перевірка роботи комп’ютерної системи

Для перевірки функціональності комп'ютерної системи ми будемо проводити такі дії:

– перевіримо доступність вузлів мережі між собою;

– перевіримо роботу HTTP серверу з відкритою сторінкою відомостей про кваліфікаційну роботу;

– перевіримо SSH підключення до комутатора;

– перевіримо зв'язок між вузлами з різних VLAN при автоматичному призначенні адрес.

– перевіримо динамічне призначення IP-адрес для вузлів у VLAN-ах за допомогою DHCP.

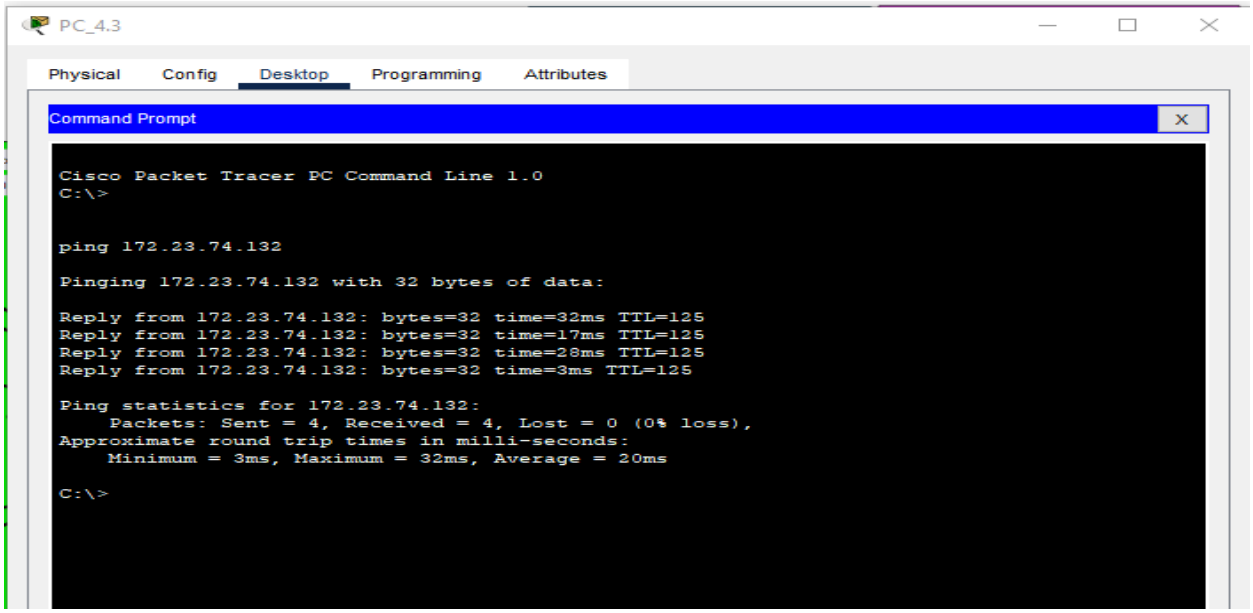

Рисунок 3.6 – Ехо-запит з відділу «Відділу технічної підтримки» до «Відділу якості продукції»

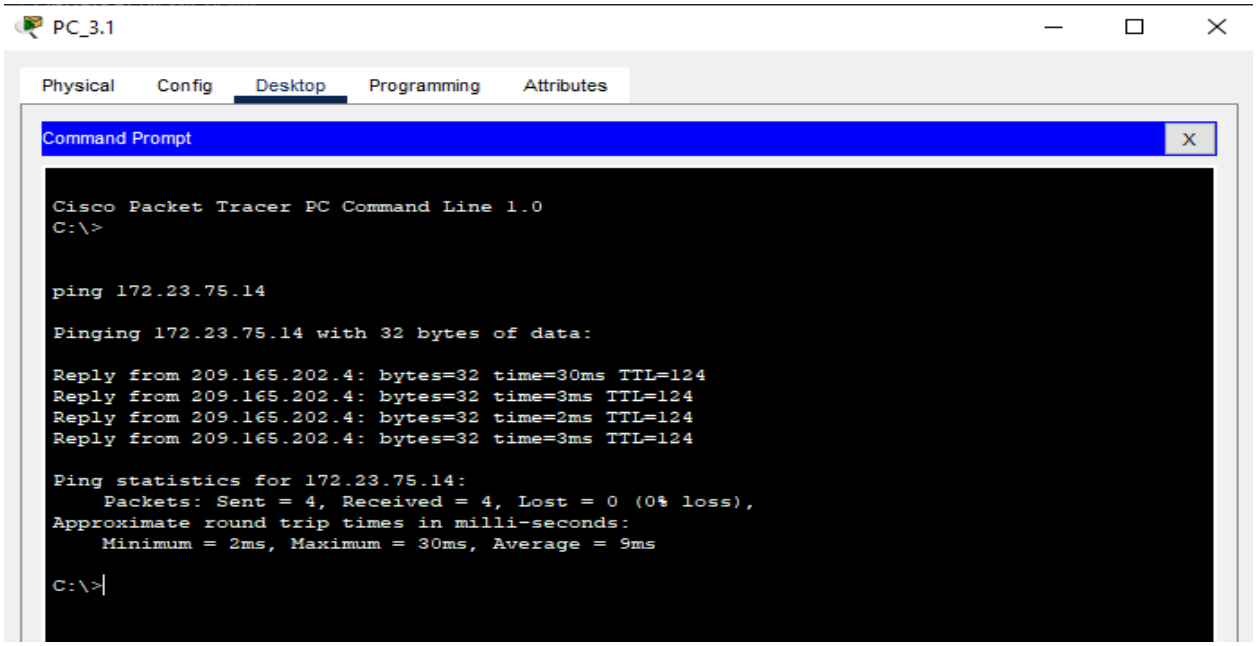

Рисунок 3.7 – Ехо-запит з віддаленої мережі до HTTP серверу.

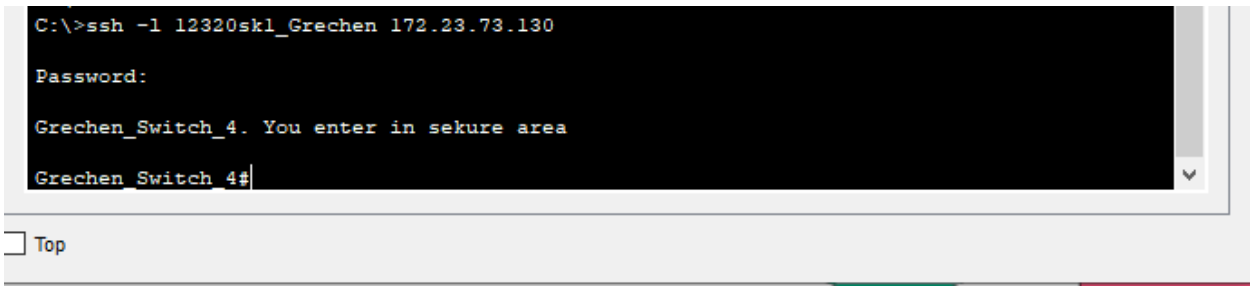

Рисунок 3.8 – Підключення по SSH до комутатора Grechen_Switch_4

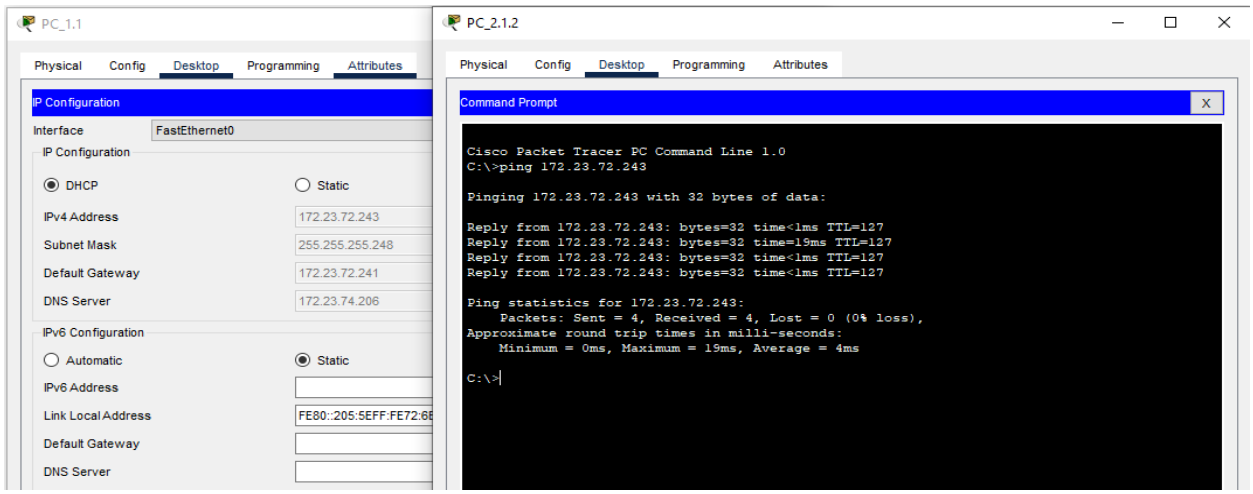

Рисунок 3.9 – Перевірка зв'язку між вузлами VLAN.

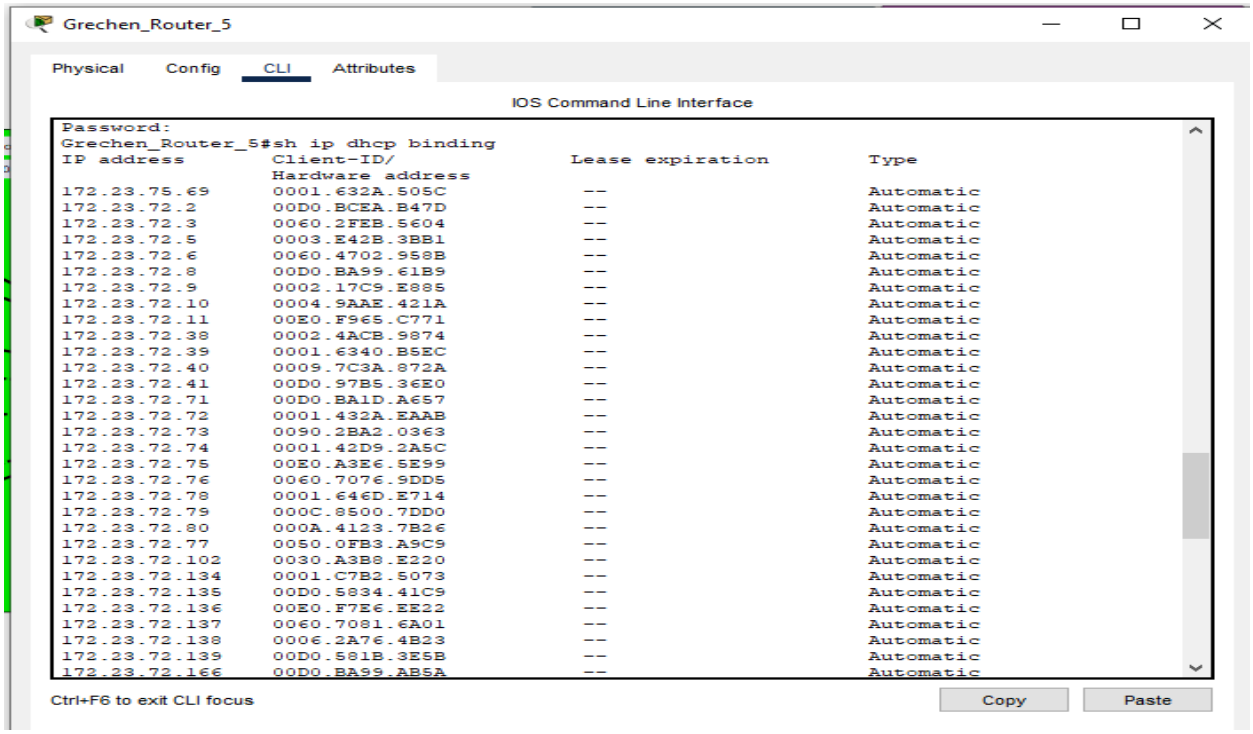

Рисунок 3.10 – Таблиця призначення IP-адрес вузлам VLAN за протоколом DHCP

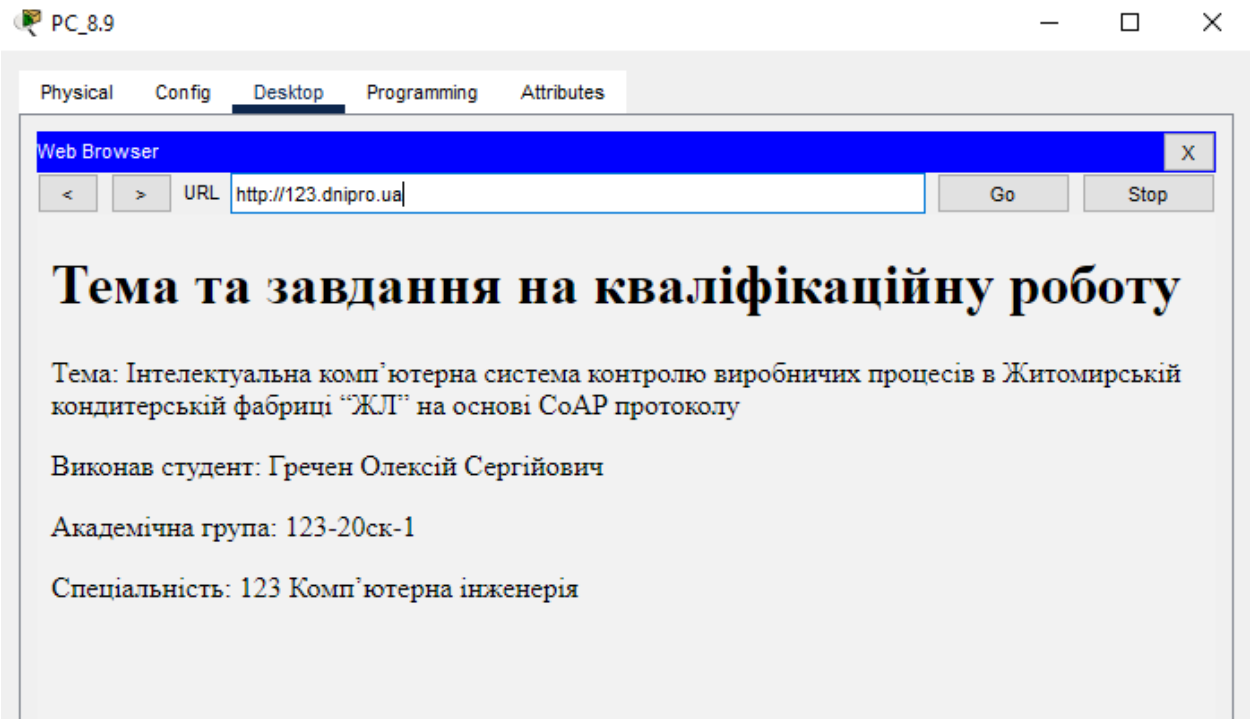

Рисунок 3.11 – Веб-сторінка з відомостями про кваліфікаційну роботу ПК «Відділу закупівель та логістики»

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Розробка інтелектуальної комп’ютерної системи контролю виробничих процесів в кондитерській фабриці “Житомирскі Ласощі” на основі CoAP протоколу

4.1.1 Детальний опис функціонування інтелектуальної комп’ютерної системи контролю виробничих процесів

В інтелектуальній комп’ютерній системі контролю виробничих процесів буде такий функціонал:

– на підприємствах де виробляються продукти харчування, а саме у робочих зонах, не повинні буди по сторонні люди, тому щоб забезпечити безпеку готового продукту, на вході в кожен виробничий цех, буде встановлений контрольно-пропускний пункт по чипованим ID-карткам та турникетом. Також таке рішення забезпечить зникненню готової продукції з цехів виробництва, тому що співробітники будуть починати робочий день проходивши через цей контроль-пропускний пункт, так і завершуючи робочий день, виходячи з цеху через цей контрольно-пропускний пункт;

– для покращенню безпеки виробничих приміщень, а також для моніторингу за виробничими процесами, буде встановлено відеокамери. Це забезпечить підприємство відеозаписами в разі випадків проникнення або завдаванню шкоди обладнанню;

– для забезпечення безпеки від пожежі, у кожен виробний цех кондитерської фабрики буде встановлено противо-пожежна сигналізація, датчик виявлення пожежі та сплинкери. Це забезпечить безпеку для обладнання та співробітників у разі виникнення пожежі;

– у виробничих цехах харчової продукції завжди повинно бути якісне повітря, стабільної температури, вологості та без вмісту вуглекислого газу.

Щоб забезпечити контроль якості повітря у виробничих цехах кондитерської фабрики буде встановлена інтелектуальна комп’ютерна система контролю якості повітря. Це буду три датчики та вентиляція.

Інтелектуальна комп’ютерна система буде оновлювати постійно інформацію з датчиків та вмикати в разі чого роботу вентиляції завдяки контролеру обладнання;

– одним із важливих об'єктів на підприємствах з виробництву харчової продукції, це виробничі лінії. Буває так що вони ламаються, тому для забезпечення швидкого реагування, на виробничу лінію буде встановлений датчик для фіксування руху, якщо виробнича лінія зупиниться у оператора в кабінеті загориться сигнальна лампочка про несправність, після цього спеціалісти з технічного відділу швидко будуть проінформовані про несправність.

4.1.2 Вибір основних пристроїв інтелектуальної комп’ютерної системи контролю виробничих процесів

Для реалізації описаного функціоналу інтелектуальної комп'ютерної системи контролю виробничих процесів на кондитерській фабриці “Житомирські Ласощі “ будуть використані наступні пристрої:

Контрольно-пропускний пункт буде забезпечений RFID-турникетом такої моделі: TRIPOD SECURITY TURNSTILE GATE MT156

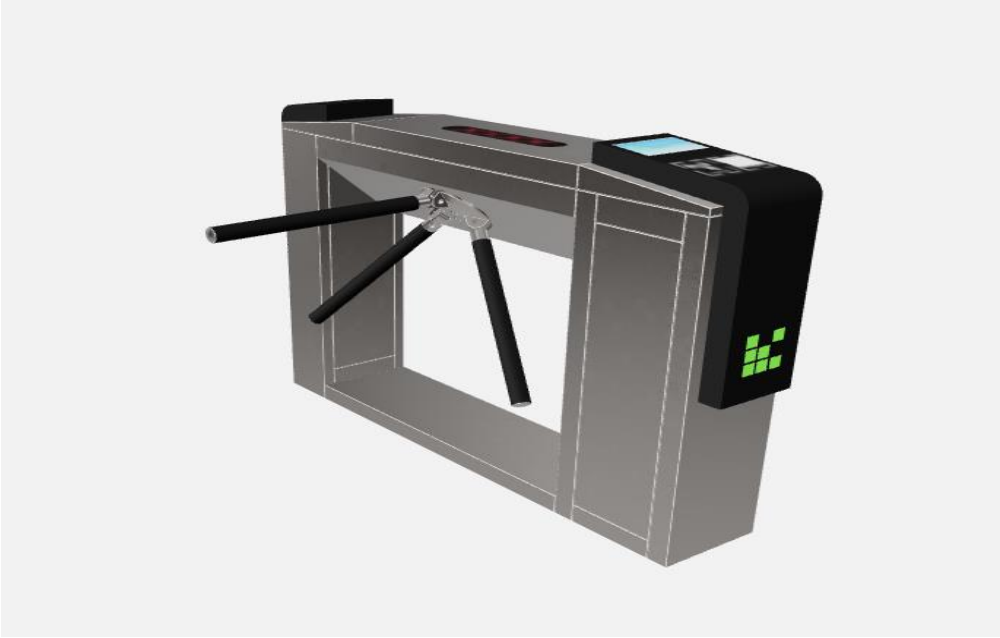

Рисунок 4.1 – Зображення 3D моделі турнікету TRIPOD SECURITY TURNSTILE GATE MT156

Точні характеристики турнікету:

– розмір: 480*280*980 мм;

– ширина смуги руху: 550 мм;

– швидкість проходження: 35 осіб / хв.;

– джерело живлення: 110 В / 220 В 50/60 Гц 5. Вага: 40 кг;

– сигнал відкриття воріт: сухий контакт / реле;

– матеріал корпусу: нержавіюча сталь 304;

– надійність механізму: 3 мільйони, несправностей немає;

– матеріал рукоятки: нержавіюча сталь 304.

Відеоспостереження в виробничих цехах буде забезпечено відеокамерами зі здатністю до запису Hikvision DS-2CD1021-I(F).

Точні характеристики відеокамер:

– матриця: 1/2.7" CMOS;

– мін. чутливість: колір: 0.01 лк(F2.0, AGC вкл), Ч/Б: 0 лк з ІЧ;

– швидкість затвора: 1/3 - 1/100, 000 с;

– повільна витримка затвора: Підтримує;

– фокусна відстань: 4 мм;

– кути огляду: Г: 90°, В: 48°, Д: 107°;

– тип підсвічування: ІЧ;

– дальність підсвічування: 30 м;

– відео компресія: H.264;

– відео бітрейт: 32 кбіт/с - 8 мбіт/с;

– макс. роздільна здатність: 1920 × 1080;

– кількість потоків: 2;

– частота кадрів (головний потік): 1920 × 1080, 1280 × 720 25 к/с;

– частота кадрів (доп. потік): 640 × 480, 640 × 360 25 к/с;

– метод зберігання: FTP;

– мережеві протоколи: TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP™, SMTP, IGMP, 802.1X, QoS, IPv6, Bonjour, IPv4, UDP, SSL/TLS;

– програмне забезпечення: iVMS-4200, Hik-Connect;

– кількість одночасних підключень: 6;

– мережеві інтерфейси: 1 RJ45, 10M/100M;

– живлення: 12В DC, 0.4 А;

– PoE: 802.3af, 36 В to 57 В;

– споживана потужність: 5 Вт;

– робоча температура: -30 °С - 60 °С;

– ступінь захисту: IP67;

–матеріал: метал+пластик.

Рисунок 4.2 – Зображення відеокамерим моделі Hikvision DS-2CD1021-I(F).

Противопожежна система у виробничих цехах буде встановлена Siemens Cerberus PRO, вона в себе включає датчики виявлення пожежі та контроль над сплинкерами, включаючи функцію PoE-підключення. Ці системи володіють передовими функціями детекції пожежі, інтелектуальним аналізом даних і потужною системою управління, що

дозволяє оперативно реагувати на пожежні ситуації. Датчик виявлення пожежі буде такий OH720. Та сплинкери ZSTDY-15.

Рисунок 4.3 – Зображення датчику виявлення пожежі QH720.

Точні характеристики датчику виявлення пожежі:

– стандарт: CEA 4021 , EN 54-7 , EN 54-17;

– категорія захисту: IP40; IP42 з ущільненням основи детектора;

– робоча напруга: 12...33 В постійного струму;

– робоча температура: -10...55 °C;

– температура зберігання: -30...+70 °C;

– струм спокою: ~230 мкА;

– зовнішній індикатор тривоги: 2;

– сумісність з системою: C-NET -> FS720;

– протокол зв'язку: C-NET;

– відносна вологість: відносне значення ≤ 95%;

– допустима швидкість повітря: 5 м / сек.

Інтелектуальна комп’ютерна система контролю якості повітря буде складатися з трьох датчиків, контролером та самої вентиляції:

– датчик вологості HIH-4000:

Точні характеристики датчику вологості:

– діапазон вимірювання вологості: 0-100% (абсолютна вологість);

– точність вимірювання вологості: ±3% (при 25 °C);

– температурний діапазон: -40 °C до +85 °C;

– вихідний сигнал: аналоговий;

– інтерфейс: 3-провідний (VCC, GND, аналоговий вихід);

– живлення: 4.75-5.5 В постійного струму.

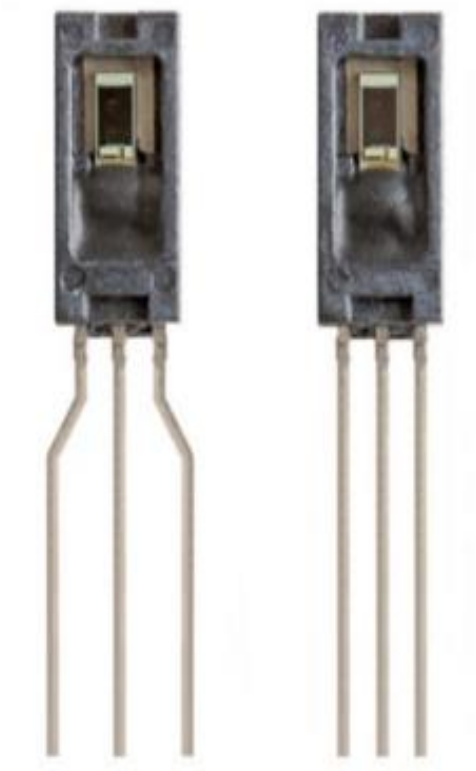

Рисунок 4.4 – Зображення датчику вологості HIH-4000

Датчик температури TMP36:

Точні характеристики датчику температури:

– діапазон вимірювання температури: -40 °C до +125 °C;

– точність вимірювання температури: ±2 °C;

– вихідний сигнал: аналоговий;

– інтерфейс: 3-провідний (VCC, GND, аналоговий вихід);

– живлення: 2.7-5.5 В постійного струму.

Рисунок 4.5 – Зображення датчику температури TMP36

Датчик вуглекислого газу MQ-7:

Точні характеристики датчику вуглекислого газу:

– діапазон вимірювання концентрації CO2: 20 ppm до 2000 ppm;

– вихідний сигнал: аналоговий;

– інтерфейс: 3-провідний (VCC, GND, аналоговий вихід);

– живлення: 5 В постійного струму;

– чутливість: 0.2-0.4 V/ppm CO2;

– витрата струму: менше 150 мА.

Рисунок 4.6 – Зображення датчику MQ-7

– контролер обладнання Raspberry Pi 4 Model B 8 GB

Точні характеристики контролеру:

– RAM: 8 GB;

– процесор: BROADCOM BCM2711;

– кількість ядер процесора: 4;

– харчування: 5V 3A;

– бездротові можливості: Bluetooth;

– кількість GPIO контактів: 40 pins;

– частота процесора: 1.5 ГГц;

– інтерфейси: 3.5 Jack, RJ45, USB, microHDMI;

– мережеві можливості: Ethernet 10/100/1000, WiFi 2.4G/5.8G 300 mb/s;

– сховище eMMC, microSD;

– кількість USB-портов, 4.

Рисунок 4.7 – Зображення контролеру обладнання Raspberry Pi 4 Model B 8 GB

Для контролю руху виробничої лінії буде встановлений лазерний датчик SICK M4000 Advanced та сигнальна лампа Werma Signaltechnik 890 Series в кабінеті оператора.

Точні характеристики датчику SICK M4000 Advanced:

– принцип роботи: SICK M4000 Advanced використовує лазерне випромінювання для сканування простору і виявлення об'єктів;

– зони безпеки: Сканер дозволяє налаштовувати декілька зон безпеки, що дозволяє створювати пристрої з різними рівнями обмежень доступу для безпечної роботи;

– швидкість відновлення: SICK M4000 Advanced може оперативно сканувати простір і виявляти перешкоди з високою швидкістю в режимі реального часу;

– висока надійність: Цей пристрій відомий своєю стійкістю до шумів, впливу віддзеркалюючих поверхонь та високих рівнів освітлення, що робить його надійним для використання у вимогливих промислових умовах;

– інтерфейси: SICK M4000 Advanced підтримує різні інтерфейси для підключення та комунікації, такі як Ethernet, RS-485, CAN і т. д;

– конфігурація: Сканер може бути налаштований за допомогою спеціального програмного забезпечення для відповідності конкретним вимогам безпеки і просторових обмежень.

Рисунок 4.8 – Зображення датчику SICK M4000 Advanced

Таблиця 4.1 – Специфікація обладнання

Позиція	Найменування	Марка	Одиниця вимірювання	Кількість
1	Турнікет з RFID зчитувачем TRIPOD SECURITY TURNSTILE GATE MT156	TRIPOD	шт.	7
2	Відеокамера Hikvision DS-2CD1021-I(F)	Hikvision	шт.	42
3	Датчик виявлення пожежі QH720	Siemens	шт.	7
4	Протипожежна система Siemens Cerberus PRO	Siemens	шт.	7
5	Датчик вологості HIH-4000	Honeywell	шт.	7
6	Датчик температури TMP36	Analog Devices	шт.	7
7	Датчик вуглекислого газу MQ-7	Analog Devices	шт.	7
8	Контролер обладнання Raspberry Pi 4 Model B 8 GB	Raspberry	шт.	7
9	Датчик руху лазерний SICK M4000 Advanced	SICK	шт	7

Ці пристрої були вибрані згідно технічних вимог.

4.1.3 Розробка переліку вхідних та вихідних сигналів і даних

Для контролеру Raspberry Pi 4 Model B 8 GB було розроблено дві таблиці:

Таблиця 4.2 – Вхідні сигнали

Найменування інформації	Іден-тифі-катор	Напр. вх./вих.	Функція	Вид	Джерело/ отримувач	Форма подання		Період вв./вив., сек.
Температура	TEMP	Вхід	Вимірювання температури	Аналог. сигнал	Датчик температури	4/20 мА	4 байта	1
Дим	SMOKE	Вхід	Вимірювання рівня диму	Аналог. сигнал	Датчик диму	4/20 мА	4 байта	1

Продовження таблиці 4.2

Вологість	HUM	Вхід	Вимірювання вологості	Аналог. сигнал	Датчик вологості	4/20 мА	4 байта	1

Таблиця 4.3 – Вихідні сигнали

Найменування інформації	Ідентифікатор	Напр. вх./вих.	Функція	Вид	Джерело/ отримувач	Форма подання		Період вв./вив., сек.
Стан системи	SYSTEM_STATE	Вихід	Керування режимами	Лог. сигнал	Контролер	Лог. значення	Змінний	4

4.1.4 Розробка принципової схеми керуючого обладнання інтелектуальної комп’ютерної системи контролю якості повітря

Структурна та принципова схема керуючого обладнання Raspberry Pi 4 Model B 8 GB показують нам детально компоненти обладнання та роз’єми для підключень. Принципова схема показує принцип роботи системи без врахування деталей реалізації. Вона дозволяє сконцентруватись на логіці та функціональності системи, допомагає при аналізі та оптимізації.

Структурна схема допомагає візуалізувати фізичну архітектуру системи, показуючи, як її компоненти організовані і зв'язані між собою. Це може бути корисно при проектуванні, розумінні та аналізі системи.

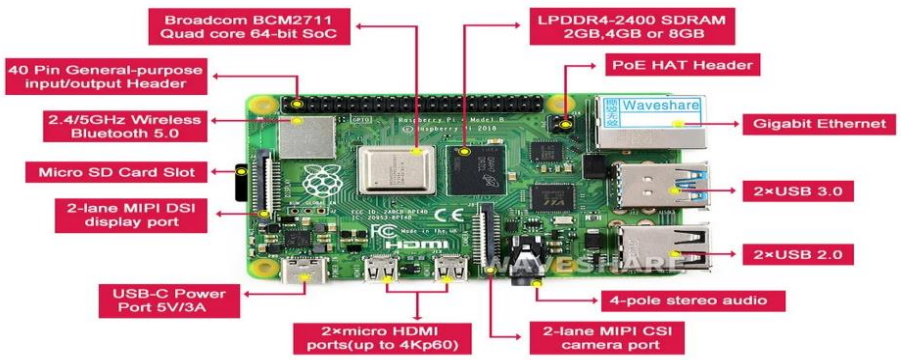

Рисунок 4.9 – Структурна схема керуючого обладнання Raspberry Pi 4 Model B 8 GB

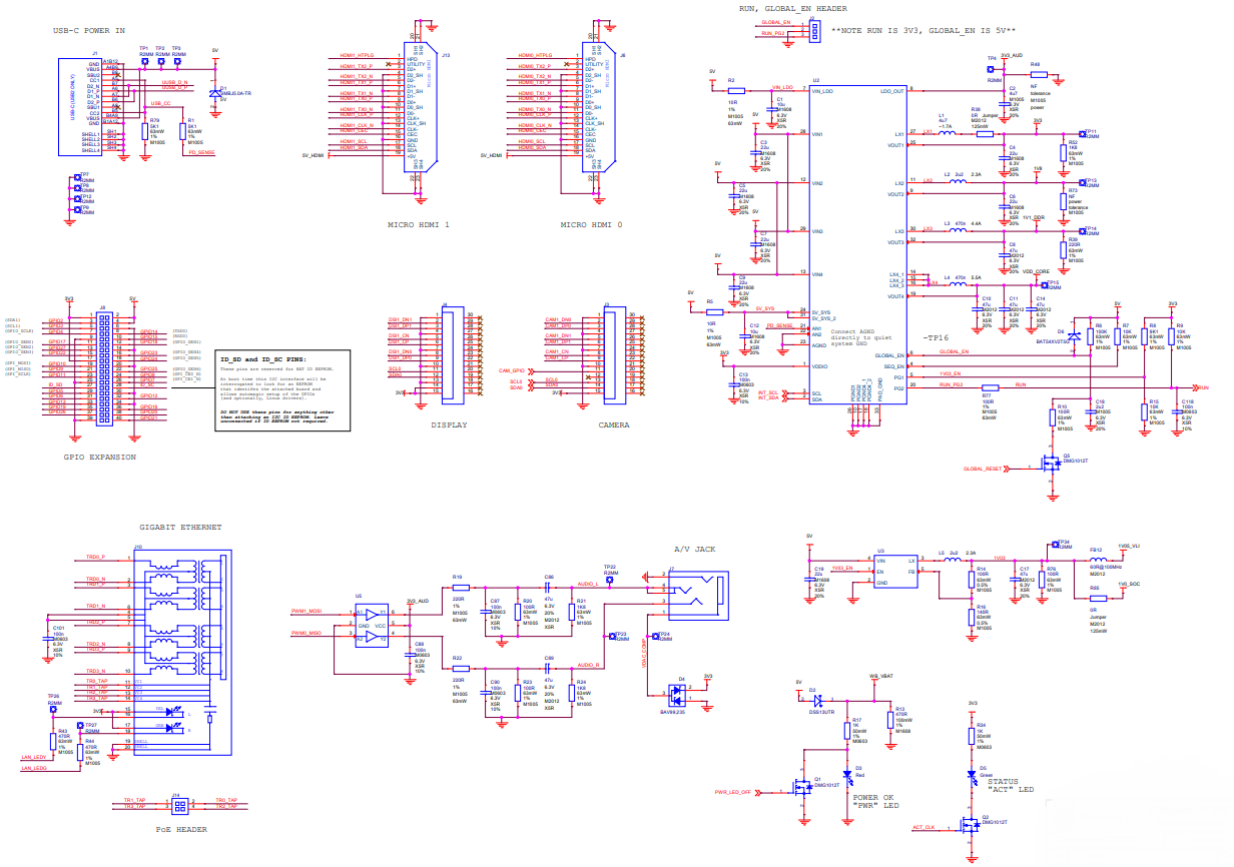

Рисунок 4.10 – Принципова схема керуючого обладнання Raspberry Pi 4 Model B 8 GB

4.1.5 Налаштування керуючого обладнання інтелектуальної комп'ютерної системи контролю якості повітря

Для контролеру Raspberry Pi 4 Model B 8 GB була розроблена програма на мові програмування Python для забезпеченню контролю інтелектуальної комп'ютерної системи контролю якості повітря у виробничих цехах харчової продукції. Контролер будет збирати дані з датчків у виробничих цехах та передавати дані на IoT або CoAP сервер.

Програма на мові Python:

*from gpio import **

*from time import **

*from ioeclient import **

```
def main():
    pinMode(0, OUT)
    pinMode(1, OUT)
    pinMode(2, OUT)
    temp = 25
    co = 0.15
    max_humidity = 50

    IoEClient.setup({
        "type": "air quality control",
        "states": [{
            "name": "Smoke",
            "type": "number",
        },
        {
            "name": "Temperature",
            "type": "number"
        },
        {
            "name": "Humidity",
            "type": "number"
        }]
    })

    while True:
        temperature = (((analogRead(A0) - 0) * (100 - -100)) / (1023 - 0)) + -
100
        smoke = (analogRead(A2)/ 10)
        humidity = (analogRead(A1)/ 10)
```

```
        if temperature > co or smoke > temp or humidity > max_humidity:
            customWrite(0, 2)
            customWrite(1, 2)
            customWrite(2, 2)
        else:
            customWrite(0, 0)
            customWrite(1, 0)
            customWrite(2, 0)

        IoEClient.reportStates([smoke, temperature, humidity])

        delay(100)

if __name__ == "__main__":
    main()
```

4.1.6 Налаштування IoT серверу інтелектуальної комп'ютерної системи контролю виробничих процесів

Моніторинг за інтелектуальною комп'ютерною системою виробничих процесів в кондитерській фабриці "Житомирські Ласощі" відбувається завдяки IoT серверу.

Таблиця 4.4 – Розроблені сценарії на IoT-сервері

Назва сценарію	Умова	Дії
Antifire_1.1.1_on	Fire_datch_1.1.1 Fire Detected is true	Set Spr_1.1.3 Status to true Set Spr_1.1.1 Status to true Set Spr_1.1.2 Status to true
Antifire_1.1.1_off	Fire_datch_1.1.1 Fire Detected is false	Set Spr_1.1.3 Status to false Set Spr_1.1.1 Status to false Set Spr_1.1.2 Status to false
Line_control_1.1.1_on	M_sensor_1.1.1 On is true	Set Siren_1.1.1 On to false
Line_control_1.1.1_off	M_sensor_1.1.1 On is false	Set Siren_1.1.1 On to true

Продовження таблиці 4.4

Antifire_2.1.1_on	Fire_datch_2.1.1 Fire Detected is true	Set Spr_2.1.3 Status to true Set Spr_2.1.2 Status to true Set Spr_2.1.1 Status to true
Antifire_2.1.1_off	Fire_datch_2.1.1 Fire Detected is false	Set Spr_2.1.3 Status to false Set Spr_2.1.2 Status to false Set Spr_2.1.1 Status to false
Line_control_2.1.1_on	M_sensor_2.1.1 On is true	Set Siren_2.1.1 On to false
Line_control_2.1.1_off	M_sensor_2.1.1 On is false	Set Siren_2.1.1 On to true
Antifire_3.1.1_on	Fire_datch_3.1.1 Fire Detected is true	Set Spr_3.1.1 Status to true Set Spr_3.1.2 Status to true Set Spr_3.1.3 Status to true
Antifire_3.1.1_off	Fire_datch_3.1.1 Fire Detected is false	Set Spr_3.1.1 Status to false Set Spr_3.1.2 Status to false Set Spr_3.1.3 Status to false
Line_control_3.1.1_on	M_sensor_3.1.1 On is true	Set Siren_3.1.1 On to false
Line_control_3.1.1_off	M_sensor_3.1.1 On is false	Set Siren_3.1.1 On to true
Antifire_4.1.1_on	Fire_datch_4.1.1 Fire Detected is true	Set Spr_4.1.3 Status to true Set Spr_4.1.2 Status to true Set Spr_4.1.1 Status to true
Antifire_4.1.1_off	Fire_datch_4.1.1 Fire Detected is false	Set Spr_4.1.3 Status to false Set Spr_4.1.2 Status to false Set Spr_4.1.1 Status to false
Line_control_4.1.1_on	M_sensor_4.1.1 On is true	Set Siren_4.1.1 On to false
Line_control_4.1.1_off	M_sensor_4.1.1 On is false	Set Siren_4.1.1 On to true
Antifire_5.1.1_on	Fire_datch_5.1.1 Fire Detected is true	Set Spr_5.1.2 Status to true Set Spr_5.1.3 Status to true Set Spr_5.1.1 Status to true
Antifire_5.1.1_off	Fire_datch_5.1.1 Fire Detected is false	Set Spr_5.1.2 Status to false Set Spr_5.1.3 Status to false Set Spr_5.1.1 Status to false
Line_control_5.1.1_on	M_sensor_5.1.1 On is true	Set Siren_5.1.1 On to false
Line_control_5.1.1_off	M_sensor_5.1.1 On is false	Set Siren_5.1.1 On to true
Antifire_6.1.1_on	Fire_datch_6.1.1 Fire Detected is true	Set Spr_6.1.1 Status to true Set Spr_6.1.2 Status to true Set Spr_6.1.3 Status to true
Antifire_6.1.1_off	Fire_datch_6.1.1 Fire Detected is false	Set Spr_6.1.1 Status to false Set Spr_6.1.2 Status to false Set Spr_6.1.3 Status to false
Line_control_6.1.1_on	M_sensor_6.1.1 On is true	Set Siren_6.1.1 On to false
Line_control_61.1_off	M_sensor_6.1.1 On is false	Set Siren_6.1.1 On to true

Продовження таблиці 4.4

Antifire_7.1.1_on	Fire_datch_7.1.1 Fire Detected is true	Set Spr_7.1.2 Status to true Set Spr_7.1.1 Status to true Set Spr_7.1.3 Status to true
Antifire_7.1.1_off	Fire_datch_7.1.1 Fire Detected is false	Set Spr_7.1.2 Status to false Set Spr_7.1.1 Status to false Set Spr_7.1.3 Status to false
Line_control_7.1.1_on	M_sensor_7.1.1 On is true	Set Siren_7.1.1 On to false
Line_control_7.1.1_off	M_sensor_7.1.1 On is false	Set Siren_7.1.1 On to true
Kontrol_rfid_1.1.1_valid	Reader_1.1.1 Card ID = 1001	Set Reader_1.1.1 Status to Valid
Kontrol_rfid_1.1.1_invalid	Reader_1.1.1 Card ID != 1001	Set Reader_1.1.1 Status to Invalid
Kontrol_rfid_2.1.1_valid	Reader_2.1.1 Card ID = 1002	Set Reader_2.1.1 Status to Valid
Kontrol_rfid_2.1.1_invalid	Reader_2.1.1 Card ID != 1002	Set Reader_2.1.1 Status to Invalid
Kontrol_rfid_3.1.1_valid	Reader_3.1.1 Card ID = 1003	Set Reader_3.1.1 Status to Valid
Kontrol_rfid_3.1.1_invalid	Reader_3.1.1 Card ID != 1003	Set Reader_3.1.1 Status to Invalid
Kontrol_rfid_4.1.1_valid	Reader_4.1.1 Card ID = 1004	Set Reader_4.1.1 Status to Valid
Kontrol_rfid_4.1.1_invalid	Reader_4.1.1 Card ID != 1004	Set Reader_4.1.1 Status to Invalid
Kontrol_rfid_5.1.1_valid	Reader_5.1.1 Card ID = 1005	Set Reader_5.1.1 Status to Valid
Kontrol_rfid_5.1.1_invalid	Reader_5.1.1 Card ID != 1005	Set Reader_5.1.1 Status to Invalid
Kontrol_rfid_6.1.1_valid	Reader_6.1.1 Card ID = 1006	Set Reader_6.1.1 Status to Valid
Kontrol_rfid_6.1.1_invalid	Reader_6.1.1 Card ID != 1006	Set Reader_6.1.1 Status to Invalid
Kontrol_rfid_7.1.1_valid	Reader_7.1.1 Card ID = 1007	Set Reader_7.1.1 Status to Valid
Kontrol_rfid_7.1.1_invalid	Reader_7.1.1 Card ID != 1007	Set Reader_7.1.1 Status to Invalid

4.1.7 Демонстрація CoAP зв’язку між пристроями інтелектуальної комп’ютерної системи контролю виробничих процесів

У Cisco Packet Tracer нажаль реалізація CoAP протоколу відсутня, тому реалізувати роботу цього протоколу для роботи інтелектуальної комп’ютерної системи контролю виробничих процесів, але буде наведена схема роботи протоколу CoAP.

У протоколі CoAP взаємодія між клієнтом і сервером базується на логіці "клієнт-сервер". Сервер забезпечує доступ до своїх ресурсів за певною адресою, а клієнти можуть звертатися до цієї адреси за допомогою стандартних HTTP-методів, таких як:

– GET (отримати ресурс);

– POST (створити ресурс);

– PUT (оновити ресурс);

– DELETE (видалити ресурс).

Протокол CoAP використовує спеціальний формат повідомлень, який є легким і оптимізованим для використання в ресурсом обмежених мережах. Він використовує UDP (User Datagram Protocol) як транспортний протокол і працює на портах 5683 (незашифрований) і 5684 (зашифрований з використанням DTLS).

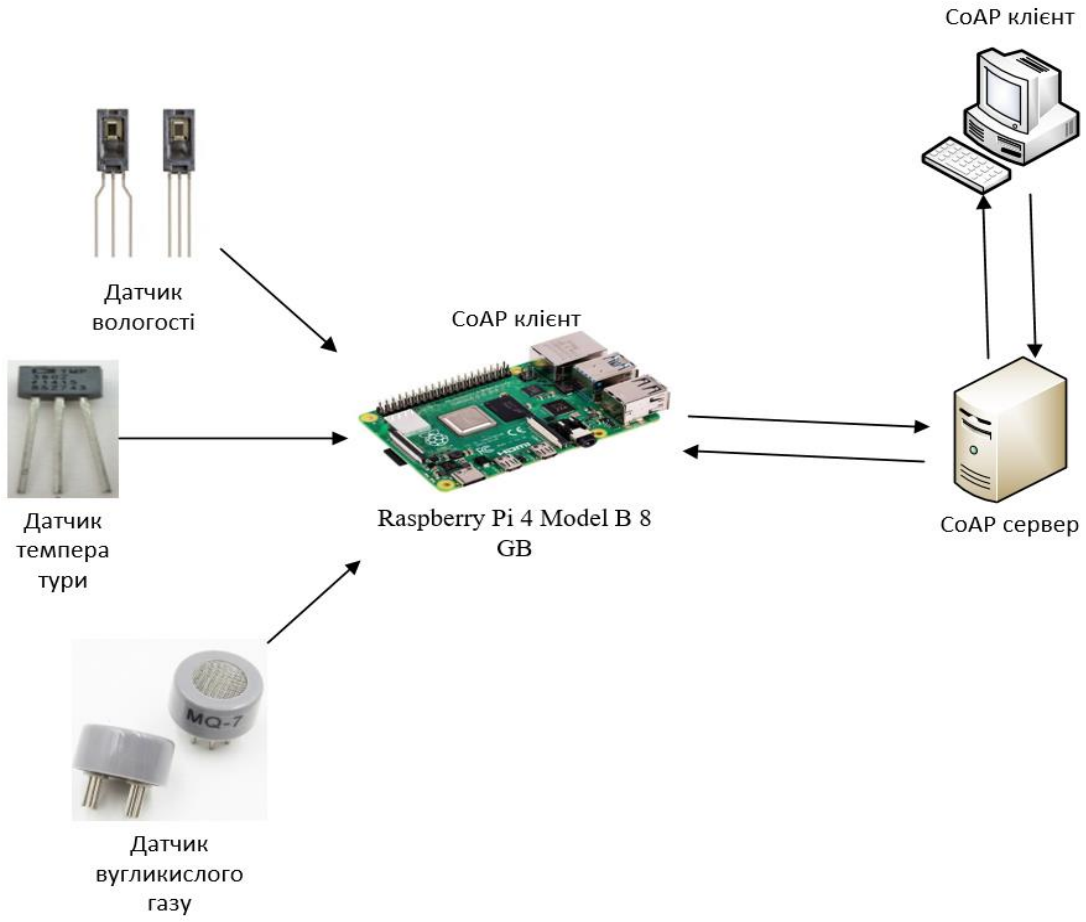

Рисунок 4.11 – Зображення роботи взаємодії CoAP протоколу

Також для реалізації зв’зку CoAP протоколу на CoAP сервері та у CoAP клієнта повинні бути програми налаштувань, буде наведено приклад реалізації на мові програмування Python:

Для серверу:

from coapthon.server.coap import CoAP

from exampleresources import BasicResource

```
class CoAPServer(CoAP):
    def __init__(self, host, port):
        CoAP.__init__(self, (host, port))
        self.add_resource('basic/', BasicResource())

def main():
    server = CoAPServer("0.0.0.0", 5683)
    try:
        server.listen(10)
    except KeyboardInterrupt:
        print "Server Shutdown"
        server.close()
        print "Exiting..."

if __name__ == '__main__':
    main()
```

Також потрібно додати деякі ресурси для серверу:

```
from coapthon.resources.resource import Resource

class BasicResource(Resource):
    def __init__(self, name="BasicResource", coap_server=None):
        super(BasicResource, self).__init__(name, coap_server, visible=True,
        observable=True, allow_children=True)
        self.payload = "Basic Resource"

    def render_GET(self, request):
```

```
        return self

    def render_PUT(self, request):
        self.payload = request.payload
        return self

    def render_POST(self, request):
        res = BasicResource()
        res.location_query = request.uri_query
        res.payload = request.payload
        return res

    def render_DELETE(self, request):
        return True
```

Для клієнта:

```
from coapthon.client.helperclient import HelperClient

host = "127.0.0.1"
port = 5683
path = "basic"

client = HelperClient(server=(host, port))
response = client.get(path)
print response.pretty_print()
client.stop()
```

В прикладі програми на мові Python показані лише базові налаштування, для більш поглибнених користувачів є ще розширені функції та інтерфейс.

4.1.8 Демонстрація роботи інтелектуальної комп’ютерної системи контролю виробничих процесів в цілому

На рисунках 4.12 – 4.18 зображена робота усіх системи у всіх виробничих цехах кондитерської фабрики “Житомирсі ласощі”

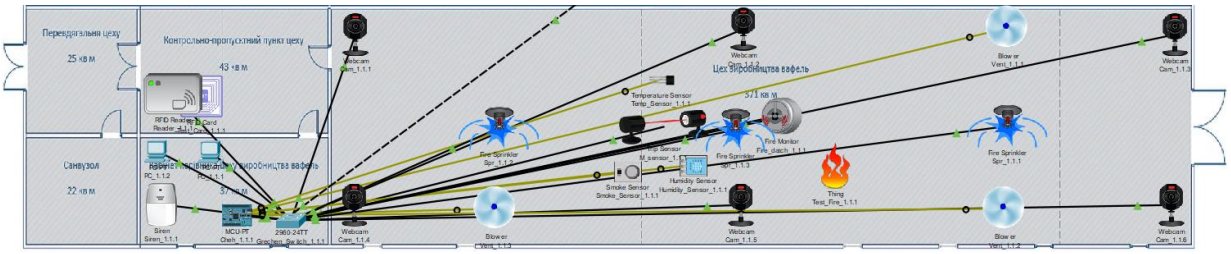

Рисунок 4.12 – Тестування систем у цеху виробництва вафель

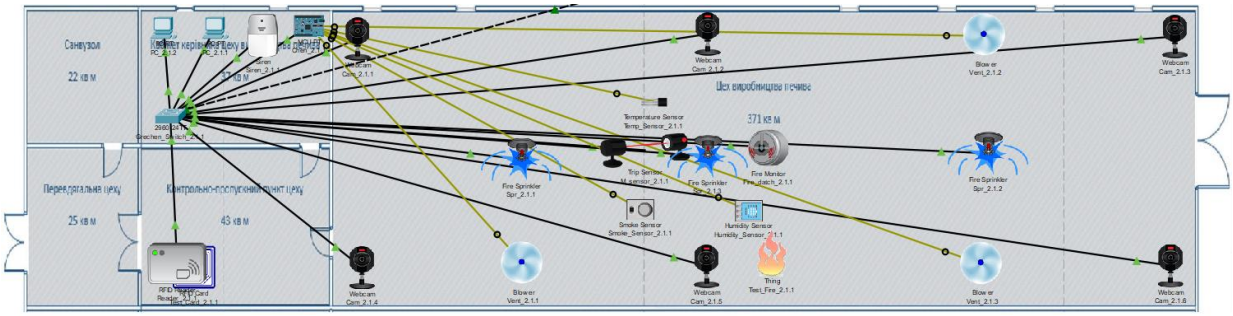

Рисунок 4.13 – Тестування систем у цеху виробництва печива

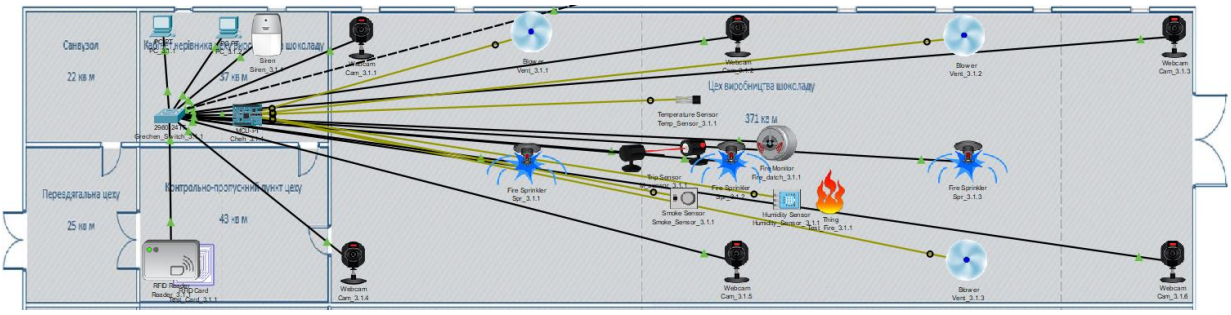

Рисунок 4.14 – Тестування систем у цеху виробництва шоколаду

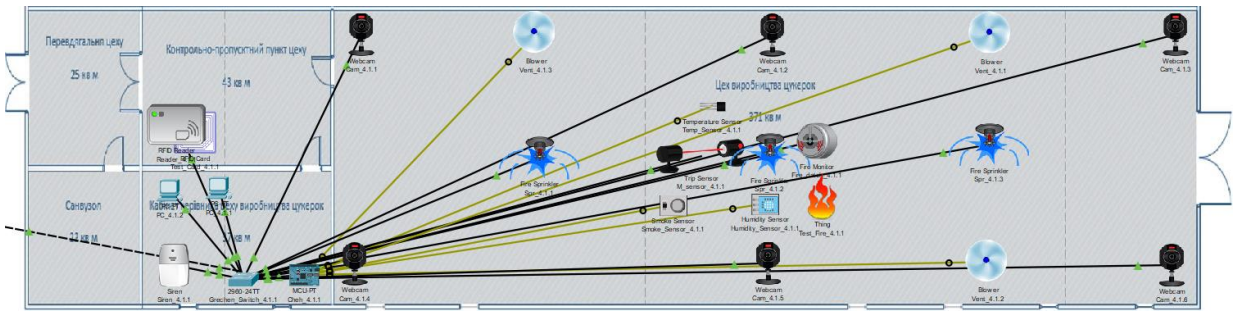

Рисунок 4.15 – Тестування систем у цеху виробництва цукерок

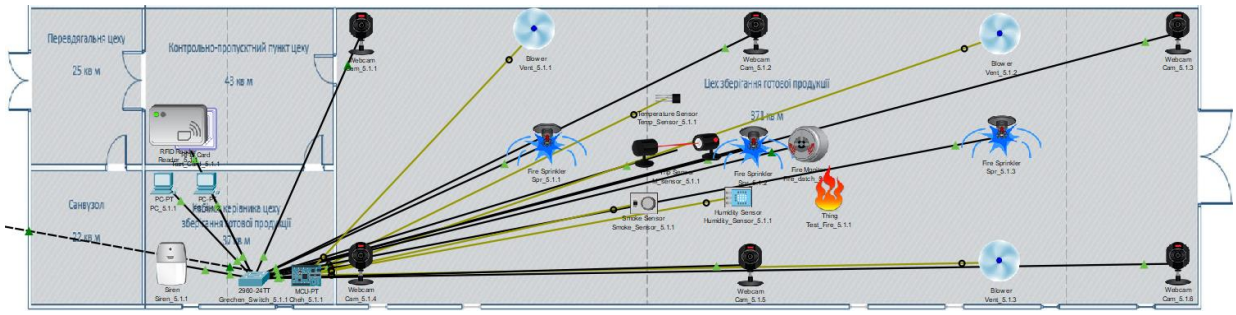

Рисунок 4.16 – Тестування систем у цеху зберігання готової продукції

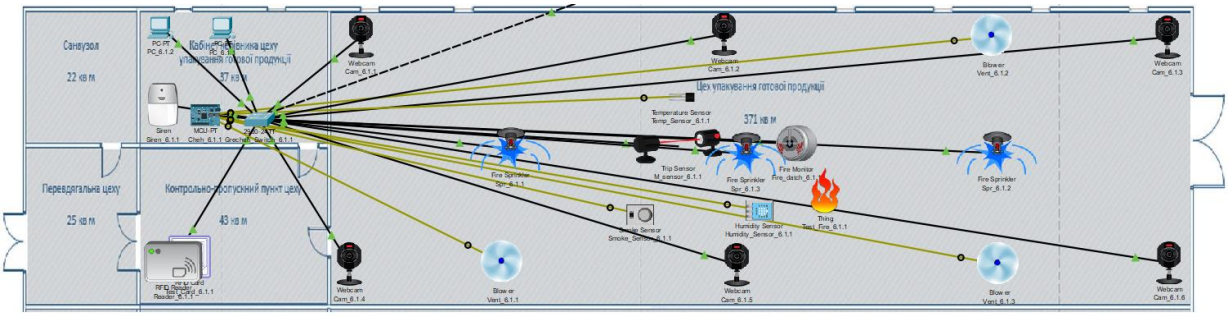

Рисунок 4.17 – Тестування систем у цеху упакування готової продукції

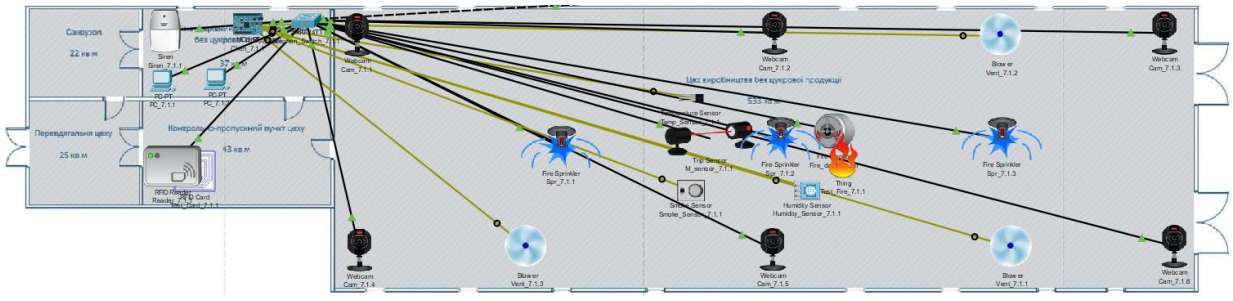

Рисунок 4.18 – Тестування систем у цеху виробництва без цукрової продукції

ВИСНОВКИ

У кваліфікаційній роботі розглядалася інтелектуальна комп’ютерна система контролю виробничих процесів на основі CoAP протоколу для кондитерської фабрики “Житомирські Ласощі”, був забезпечений відео контроль у робочих зонах, були встановленні датчики темпертур, диму, вологості у робочих зонах разом з системою контролю якості повітря та анти пожежна безпека. Також при вході до робочих цехів встановленний контрольно-пропускний пункт, щоб запобігти несанкціонованому доступу до робочих зон підприємства.

У сучасному світі модернізація промислових підприємств є дуже важливим та актуальним кроком. Технології виробництва с кожним роком розвиваються все краще, якість продукції виробленої продукції тількі покращується. Інтелектуальні комп’ютерні системи вже є майже повсюди, тому впровадження таких систем у якій промислові підприємства це дуже гарна та в майбутньому дуже продуктивна ідея. Якщо казати саме про інтелектуальні комп’ютерні системи контролю виробничих процесів, то вони здатні автоматизувати ваше підприємство, зменшити витрати електроенергії, зменшити кількість нещасних випадків в робочих зонах, зменшити кількість браку, швидко вирішувати технічні несправності. Ці всі плюси потрібні кожному великому підприємству для забезпечення належної якості виробленого продукту для своїх клієнтів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «Дніпровська політехніка», 2022.

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

3. Securing the Constrained Application Protocol (CoAP) for the Internet of Things (IoT) – Mohammed Hassan Alamri [Електронний ресурс] – Режим доступу до ресурсу: https://dspace.library.uvic.ca/bitstream/handle/1828/7996/Alamri_Mohammed_MEng_2017.pdf?sequence=1&isAllowed=y

4. Constrained Application Protocol (CoAP) [Електронний ресурс] – Режим доступу до ресурсу: https://www.ietf.org/archive/id/draft-ietf-core-coap-08.html

5. Інтернет речей (IoT) – що це таке і як працює, суть, технології і приклади. [Електронний ресурс] – Режим доступу до ресурсу: https://termin.in.ua/internet-rechey-iot/

6. Контролер Raspberry Pi 4 Model B 8 GB [Електронний ресурс] – https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

7. Network Address Translation(NAT) [Електронний ресурс] – https://medium.com/rahasak/network-address-translation-nat-df84dc1cb06c

8. Configure Basic AAA on an Access Server [Електронний ресурс] – https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

9. OSPF (Open Shortest Path First) [Електронний ресурс] – https://medium.com/geekculture/open-shortest-path-first-4c3f01de489c

10. Configure SSH on Routers and Switches [Електронний ресурс] – https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

11. IoT Cisco Virtualized Packet Core (VPC) [Електронний ресурс] – https://medium.com/@MohamedWasim001/iot-cisco-virtualized-packet-core-vpc-fb5f9e01e47f

12. VPN and Endpoint Security Clients [Електронний ресурс] – https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html

13. IPSEC VPN In Details [Електронний ресурс] – https://cyberbruharmy.medium.com/ipsec-vpn-in-details-49751bfd47e6

14. SICK | Sensor Intelligence and product portfolio [Електронний ресурс] – https://www.sick.com