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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Анікеєв Володимир Володимирович
(П.І.Б.)
академічної групи 123-19-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему Кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
кваліфікаційної роботи	проф. Нікулін С.Л.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.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

студента Анікеєв В.В. **академічної групи** 123-19-1
(прізвище, ініціали) (шифр)

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

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

на тему Кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі
(назва за наказом ректора)

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

Розділ	Зміст завдання	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	18.05.2023
Розробка апаратної частини	На основі аналізу підприємства формуються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	28.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	08.06.2023

Завдання видано _____ проф. С.Л. Нікулін
(підпис керівника) (прізвище та ініціали)

Дата видачі 04.04.2023 р.

Дата подання до атестаційної комісії 16.06.2023 р.

Прийнято до виконання _____ В.В. Анікеєв
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 95 с., 33 рис., 24 табл., 3 дод., 13 джерел.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки: кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі.

Мета: створення кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі.

У кваліфікаційній роботі бакалавра розроблена кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі.

Схема розробленої мережі у вигляді моделі ралізована на симуляторі Cisco Packet Tracer і перевірена її робота.

Перевірка та її результати описані у вигляді графіків , таблиць і наводяться у пояснювальній записці чи додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

Wi-Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

ВСТУП

Вершкове масло по суті є жиром молока. Зазвичай його готують з солодких вершків і солять. Однак традиційно він виготовляється з крему, якому дозволили відстоятися і скиснути природним шляхом. Потім вершки знімають з верхньої частини молока і переливають у дерев'яну ванну. Виготовлення вершкового масла проводиться вручну в маслобойнях. Природний процес скисання, однак, дуже чутливий, і зараження чужорідними мікроорганізмами часто псувало результат.

Сьогоднішнє комерційне виробництво вершкового масла є продуктом знань і досвіду, накопичених протягом багатьох років в таких питаннях, як гігієна, бактеріальне підкислення і термічна обробка, а також швидкого технічного розвитку, який призвів до передового обладнання, яке зараз використовується.

Основними складовими солоного вершкового масла є жир (80…82 %), вода (15,6…17,6 %), сіль кухонна (близько 2…3 %) і залишковий сир (близько 1,5 %). При виготовленні масла масляна емульсія вершків перетворюється процесом збивання в водно-масляну емульсію вершкового масла. Консистенція повинна бути однорідною, щоб вершкове масло легко розтікалося і легко тало на язику [1].

Негомогенізовані молоко і вершки містять жир в мікроскопічних кульках. Ці кульки оточені мембранами, що складаються з фосфоліпідів (емульгаторів жирних кислот) і білків, які перешкоджають об'єднанню жиру в молоці в єдину масу.

Виробка масла шляхом фізичної обробки і перемішування вершків, що пошкоджує мембрани жирних клітин і дозволяє молочним жирам з'єднуватися разом та відокремлює жир від інших частин вершків. Варіативність в способі

видобутку та виробництва впливає та дозволяє створити масла з різною консистенцією. Наприклад, масло, зібране з нового вершкового крему, містить більше кристалів жиру, тому воно більш тверде та крихке. Масло з більш старих вершків містить менше кристалів, тому воно має більш м'яку консистенцію. Крім того, спосіб, за допомогою якого масло було виготовлене, також може впливати на консистенцію. Масло містить жир у трьох формах : кристали вершкового жиру,вільний вершковий жир та неушкоджені жирові кульки.

Водяниста рідина,яка утворюється при збиванні дрібних зерен масла, плаваюча в вершках на водній основі називається пташиним молоком, хоча пташине молоко, яке найчастіше продається сьогодні, замість цього є безпосередньо ферментованим знежиреним молоком. Пташине молоко зливається; Іноді більше пташине молоко видаляють, промиваючи зерна водою. Потім зерна «опрацьовують»: пресують і розминають між собою. При ручному приготуванні це робиться за допомогою дерев'яних дошок. Це збиває вершкове масло в тверду масу і розбиває вбудовані кульки пташиного молока або води на крихітні крапельки.

Комерційне вершкове масло містить близько 80 % вершкового жиру і 15 % води. Традиційне вершкове масло може мати лише 65 % жиру і 30 % води. Вершковий жир являє собою суміш тригліцеридів, тріефіру, отриманого з гліцерину і трьох з будь-якої з декількох груп жирних кислот [2].

Комп'ютерні системи поєднані мережею здатні повністю автоматизувати і високомеханізовані технологічні операцій, що дозволяє знизити витрати молокозаводів на виробництво масла і сухих молочних продуктів.

В кваліфікаційній роботі бакалавра розроблена кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика підприємства та умов застосування КС

1.1.1 Загальні відомості

Міжнародна федерація молочних заводів (IDF) запровадила стандарт, що відноситься до масла та спреду, а саме: стандарт IDF 166:1993 «Вказівки щодо жирових спредів». Ці вказівки мають бути основою для подальшої розробки більш конкретних груп або окремих стандартів відповідно до вимог окремих країн.

Жировий спред: жировий спред – це харчовий продукт у вигляді емульсії (тип: вода в масла), що складається, в першу чергу, з водної фази та харчових жирів та масла. Харчові жири та масло: харчові продукти, що складаються, головним чином, із тригліцеридів жирних кислот. Вони можуть бути рослинного, тваринного, молочного чи морського походження. У табл. 1.1 та табл. 1.2 наведено національного законодавства може бути визначений обмежений інтервал вмісту жиру та частки молочного жиру по відношенню до інших типів жирів.

Таблиця 1.1 – Основний склад продуктів на основі молочного жиру та масла

Продукти на основі молочного жиру	Продукти на основі суміші жирів	Продукти на основі масла
Молочний жир 100%	Молочний жир мін. 15%, всього жиру макс. 80%	Молочний жир макс. всього жиру 3% всього жиру

В даний час у міжнародній торгівлі для зазначення призначення продуктів дозволені такі одиночні стандарти:

- стандарт для масла та підсировинного масла (A16 – стандарт для молочних паст з низьким вмістом жиру – проект);
- стандарт кодексу 32 – 1981 для масла;

- стандарт кодексу 13 – 1981 для мінарину.

Основною сировиною повинна бути вода та/або молочні продукти, харчові жири та/або масло або їх суміші.

Таблиця 1.2 – Найменування продуктів на основі молочного жиру та масла

Склад жиру %	Продукти на основі молочного жиру	Продукти на основі суміші жирів	Продукти на основі масла
80 – 95	Масло*	Суміш	Маргарин*
> 62 – < 80	Молочна паста	Змішана паста	Жирова паста
60 – 62	Масло с 3/4 або його зменшений склад	Суміш с 3/4 або його зменшений склад	Маргарин с 3/4 жиру або його зменшений склад
> 41 – < 60	Молочна паста або його зменшений склад	Змішана паста або його зменшений склад	Жирова паста або його зменшений склад
39 – 41	Масло с 1/2 або з низьким складом жиру	Змішана паста с 1/2 жиру або маргарин	Мінарин* с ½ або з низьким складом жиру
< 39	Молочна суміш з низьким складом жиру	Змішана паста з низьким складом жиру	Паста з низьким складом жиру

Таблиця 1.3 – Приклади жировмісних продуктів

Продукт / Состав	Масло	Маргарин	Молочна паста Бреготтс (маргарин)	Молочна паста с низьким жиром	М-кокос	Лярд
Основний матеріал	Заквашені сливки	Росл. масла и жирн.	Заквашені сливки і рослинне масло	ОМЖ* + рослинне масло + пред. конц. молоч. масла	Кокосове масло	Лярд
Жир, %	80	80	80	40	100	100
Волога, %	16-18**	≈18	17-18**	48	0	0
Соль, %	0-2	1.5-2.0	1.4-2.0	1.2	0	0
Белки, %	0.7	0.2-0.4	0.6	7.5	0	0
Удільна калорійність, кДж/100 г	3140	3100-3150	3140	1710	3900	3900
Вітаміни, М.Е./100 г	D55	D300	D300	D300	0	0
Термін зберігання при 6 – 7 °С	2-3 міс	3 міс	2-3 міс	1.5 міс	6-12 міс	6 міс
Використання	До столу, кулінарія	До столу, кулінарія	До столу, кулінарія	До столу	Кулінарія Кондитерське виробництво	Для жарки, випічка

Що стосується вмісту жиру, стандарт встановлює, що спреди на основі жирів повинні розділятися на три групи відповідно до типу жиру. Максимальний вміст жиру має становити 95 %.

Найменування продукту має бути визначено у національному законодавстві. Проте продукти мають відповідати загальним вимогам табл. 1.1, яка розрахована застосування до продуктів всіх трьох груп відповідно.

Табл. 1.1, в якій перераховані найменування, затверджене призначення та склад деяких жирових продуктів, що є у продажу у Швеції, може бути прикладом.

Протягом багатьох років була лише незначна кількість визнаних типів кулінарних жирів – наприклад, масло, маргарин, лярд та кокосове масло.

Масло та маргарин – це два продукти, на яких зосереджено основну увагу. Обидва продукти використовуються для намазування на хліб, а також у кулінарії та хлібопекарському виробництві.

В обох є недолік, що полягає в тому, що при традиційному приготуванні їх не можна легко намазувати за нормальної температури зберігання в холодильнику (+5°C). Це призвело до розробки в шістдесяті і сімдесяті роки різних запатентованих продуктів, що легко намащуються, включаючи суміші з низьким вмістом жирів (40 %), звані також мінаринами, і трохи пізніше продуктів зі зниженим вмістом жирів (60 %), званих мелларинами.

1.1.2 Масло вершкове

Масло зазвичай поділяють на дві категорії:

- солодковершкове масло (зі свіжих вершків);
- кисловершкове масло, приготовлене з бактеріальна сквашених вершків;
- масло можна також класифікувати відповідно до вмісту солі: несолоне, солоне і дуже солоне;

- до початку хіх століття масло ще виготовляли з вершків, які мали сквашуватися природним чином. потім вершки знімали з верхньої частини молока та зливали у дерев'яну діжку, масло виготовляли вручну в маслобойні.

Процес природного сквашування дуже чутливий, і потрапляння сторонніх мікроорганізмів часто псує кінцевий результат.

У міру накопичення знань про охолодження стало можливим знімати вершки до того, як вони прокиснуть, і готувати масло зі свіжих вершків. Поступово покращувалися методи, що застосовуються в маслоробстві, а також якість продукту та економічний вихід. Зрештою виявилося, що свіжі вершки можна сквашувати шляхом додавання природним чином сквашених вершків або кислої пахти. Потім з'явилася можливість здійснювати дозрівання вершкового масла у більш керованих умовах.

Винахід сепаратора (1878 р.) означало, що вершки з молока можна отримувати швидко і ефективно. Це також стало початком виробництва масла у великих масштабах. Внесок у підвищення якості продукту та економію при маслоробстві був зроблений введенням у 1890-і роки пастеризації, використанням чистих культур бактерій у 1890-х та появою на межі століть маслоробної машини.

Сучасне промислове виробництво масла є результатом застосування знань та досвіду, отриманих за багато років вивчення таких предметів, як санітарія виробництва, бактеріальне сквашування та теплова обробка, а також швидкого технічного прогресу, що надав передове обладнання, що використовується зараз.

Виробництво масла можна здійснювати партіями в маслобойні або безперервно за допомогою сучасних машин для виготовлення масла.

1.1.3 Солодковершкове та кисловершкове масло

Розкид у складі масла обумовлений особливостями виробництва окремих видів. Як видно з табл. 1.2, масло містить 80 % жиру та 16…18 % вологи, в основному залежно від того, солоне воно чи ні. В маслі також спочатку містяться вітаміни А та D.

Колір масла змінюється в залежності від вмісту каротиноїдів, які становлять від 11 до 50% загальної активності вітаміну А в молоці. Так як вміст каротиноїдів у молоці зазвичай змінюється восени і навесні, колір масла, виробленого в зимовий період, світліший. У цьому контексті можна згадати, що масло, приготована з вершків молока буйволиці, білого кольору, оскільки молоко буйволиць не містить каротиноїдів..

Рисунок 1.1 – Вершкове масло

Масло має бути щільною і мати свіжий смак. Волога, що міститься, повинна бути диспергована у вигляді дрібних крапель так, щоб масло виглядало сухим. Масло має бути однорідної консистенції, щоб її легко було намазувати і щоб воно швидко танула в роті.

Кисловершкове масло має пахнути діацетилом, а солодковершкове масло має смак вершків. У солодкого масла допускається наявність слабкого присмаку "кип'яченості".

Масло, виготовлено із сквашених вершків, має ряд переваг перед маслом зі свіжих вершків. Аромат багатший, вихід масла вищий, і після теплової обробки знижується ризик реінфекції, оскільки заквасочні культури пригнічують сторонні мікроорганізми.

Проте кисловершкове масло має свої недоліки. Пташине молоко від кисловершкового масла має набагато нижчий pH, ніж пташине молоко від масла з натуральних вершків, що часом ускладнює її утилізацію в порівнянні з солодкою пташиним молоком. Іншим недоліком кисловершкового масла є його висока чутливість до дефектів окислення, що надає продукту металевого присмаку. Ця тенденція посилюється, якщо присутні хоч найменші сліди міді чи іншого важкого металу, значно погіршується хімічна стійкість масла.

1.1.4 Виробництво масла

Традиційна ручна маслобойка, яка використовувалася раніше для домашнього приготування масла.

Спочатку масло на фермах виготовляли для домашнього використання. У ті часи використовували ручну маслобойку, показану на рис. 1.2. Після збивання та видалення пахти зерна масла збирали в дрібне корито і виробляли вручну до досягнення прийнятної сухості та структури.

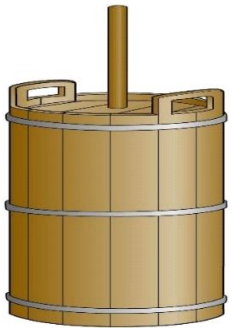


Рисунок 1.2 – Традиційна ручна маслобойка

Процеси великомасштабного виробництва масла включають велику кількість етапів, які здійснюють на сучасних молокопереробних заводах (рис. 1.3).

Рисунок 1.3 – Сучасний молокопереробний заводах

На рис. 1.4 схематично показано виробництво масла в маслоробних машинах.

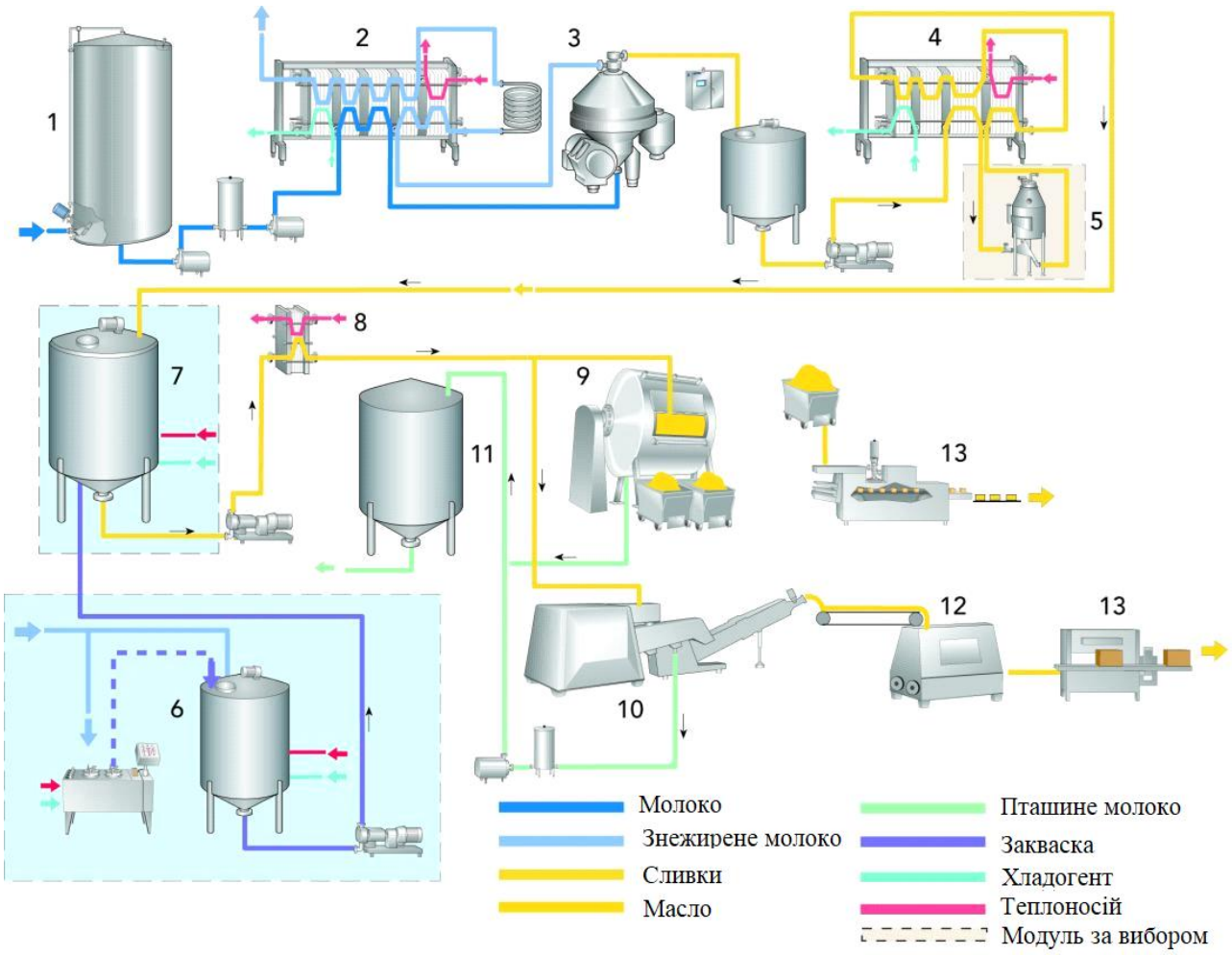


Рисунок 1.4 – Технологічна лінія з виробництва вершкового масла

Маслобойки ще використовуються, але вони швидко замінюються машинами для безперервного виробництва масла.

Вершки одержують як побічний продукт при виробництві рідких молочних продуктів або цілеспрямованим сепаруванням з незбираного молока на маслозаводі. У першому випадку вершки мають бути пастеризовані постачальником. Зберігання та постачання на маслоробний завод повинні здійснюватися таким чином, щоб не відбувалося вторинного обсіменіння, аерації або спінювання. Після процедур приймання, зважування та аналізу вершки зберігаються у танках.

Якщо вершки виробляються на маслозаводі, перед сепарацією незбиране молоко попередньо нагрівають у пастеризаторі до 63 °С. Перед подачею на

пастеризаційну установку теплі вершки направляють у танк для проміжного зберігання.

Перед перекачуванням на зберігання знежирене молоко, що надходить із сепаратора, пастеризують та охолоджують. У разі виробництва кисловершкового масла частину знежиреного молока слід використовувати для приготування закваски.

З ємності для проміжного зберігання вершки надходять на пастеризацію при температурі 95 °С або вище. Висока температура необхідна для руйнування ферментів та мікроорганізмів, які можуть погіршувати збереження масла.

Знищення небажаних мікроорганізмів також необхідне у разі виробництва масла, оскільки при цьому створюються чудові умови для розвитку культури закваски. Теплова обробка сприяє утворенню сильних антиокислювачів – сульфгідрильних сполук, які додатково знижують ризик окислення.

У лінію можна також включити вакуумну деаерацію, якщо вершки мають небажаний присмак чи запах – наприклад запах цибулі. Будь-які ароматичні сполуки будуть пов'язані з жирами та перейдуть у масло, якщо їх не видалити. Вакуумна обробка перед пастеризацією включає попередній нагрівання вершків до потрібної температури, а потім миттєве охолодження, в результаті вивільняються всі захоплені гази і леткі речовини.

Після цього вершки повертаються в пастеризатор для подальшої обробки – нагріву, витримки та охолодження – перед подачею в танк для визрівання.

У ємності для визрівання з великим об'ємом (зазвичай 30 000 л), що рекомендується, вершки піддають обробці згідно з температурною програмою, яка додасть жиру необхідну кристалічну структуру при його затвердінні під час охолодження.

Програму вибирають відповідно до таких факторів, як склад жирової фракції масла, виражений, наприклад, йодним числом, що є мірою вмісту ненасичених жирних кислот. Обробку можна також модифікувати з метою

виробництва масла з гарною консистенцією, незважаючи на низьке йодне число – наприклад, коли частка ненасичених жирних кислот низька.

Дозрівання зазвичай займає 12…15 годин. Коли це можливо, заквасувальні культури, що виробляють кислоту, додають перед термообробкою. Кількість закваски, що додається, залежить від обраної температурної програми з урахуванням йодного числа (табл. 1.3).

З ємності для дозрівання вершки подають насосом на масловиробник безперервної дії або в маслоробку. Іноді бажано проходження вершків через пластинчастий теплообмінник для отримання вершків необхідної температури. У процесі збивання масла вершки активно перемішують, щоб розбити кульки жиру, що призводить до з'єднання жиру в зерна масла. Вміст жиру в рідині, що залишилася – пташиному молоці – знижується.

Вершки поділяються на дві фракції: зерна масла та пташине молоко. У машинах з безперервним процесом маслоробства відведення пташиного молока є безперервним.

Після відведення пташиного молока масло виробляють до фази суцільного жиру з фазою тонко диспергованої води. Загальноприйнятою практикою було промивання масла після збивання водою видалення залишків пташиного молока і сухих речовин молока, але це роблять рідко. При виробництві солоного масла при безперервному виробництві сіль додають у вигляді рідини в процесі вироблення.

Після додавання солі обробку масла необхідно продовжити, щоб забезпечити рівномірний розподіл солі. Обробка масла також впливає на характеристики, за якими оцінюють продукт – аромат, смак, стійкість, зовнішній вигляд та колір. Готове масло вивантажують на блок упаковки, а звідти – на зберігання холодильник.

Таблиця 1.3 – Основні температурні програми, адаптовані до значення йодного числа, та рекомендовані обсяги закваски (у разі її використання)

Йодове число	Температурна програма, °С	Приблизна доля. закваски в %
< 28	8 – 21…20	1
28…29	8 – 21…16	2..3
30…31	8 – 20…13	5
32…24	6 – 19…12	5
35…37	6 – 17…11	6
38…39	6 – 15…10	7
> 40	20 – 8…11	5

Основні етапи виробництва кисловершкового масла періодичним та безперервним способами:

- приймання молока;
- попереднє нагрівання та пастеризація знежиреного молока;
- сепарування вершків;
- пастеризація вершків;
- вакуумна деаерація (якщо використовується);
- приготування закваски (якщо використовується);
- дозрівання та сквашування вершків (якщо використовується);
- теплова обробка;
- збивання / вироблення масла, періодичне;
- збивання / вироблення масла, безперервне;
- збір пташиного молока;
- бункер для масла зі шнековим конвеєром;
- пакувальна машина [3].

1.1.5 ПРАТ "Вінницький молочний завод "Рошен"

ПРАТ "Вінницький молочний завод "Рошен", який повністю побудований з нуля, розпочав свою виробничу діяльність у червні 2014 року. При проектуванні та будівництві підприємства були враховані всі вимоги міжнародних стандартів в сфері якості та безпечності харчових продуктів.

Рисунок 1.5 – ПРАТ "Вінницький молочний завод "Рошен"

Завод комплексно обладнано найсучаснішим обладнанням від провідного світового виробника компанії «Tetra Pak» та управляється і контролюється протягом всього виробничого процесу програмою управління виробництвом Tetra Plant Master. Всі інженерні ділянки обладнані передовими світовими агрегатами та технологіями постачання енергоресурсів.

Потужність підприємства дозволяє переробляти 600 т молока на добу. На даний час стартує друга черга модернізації, яка дозволить у найближчому майбутньому переробляти до 1 200 тон молока щодобово.

На сьогоднішній день підприємство виготовляє наступну продукцію:

- молоко сухе знежирене (Low Heat);
- молоко сухе знежирене (Medium Heat);
- молоко сухе незбиране;
- молоко сухе швидкорозчинне;

- молоко сухе карамелізоване;
- вершки сухі;
- масло солодковершкове 82,5 % жиру;
- масло кисловершкове 82,5% жиру;
- жир молочний зневоднений;
- молоко згущене.

Рисунок 1.6 – Виробничі цехи на ПРАТ "Вінницький молочний завод "Рошен"

ПРАТ "Вінницький молочний завод "Рошен" знаходиться за адресом: вул. Енергетична, 7, Вінниця 21022 Україна (рис. 1.7).

Потужність виробничих ліній дозволяє виробляти за добу до 48 т сухих молочних продуктів, до 30 т масла, до 18 т молочного жиру та до 75 т згущеного молока. На підприємстві впроваджена система управління якістю та безпечністю харчових продуктів відповідно до вимог міжнародних стандартів ISO 9001 і ISO 22000.

Рисунок 1.7 – ПРАТ "Вінницький молочний завод "Рошен"

План ПРАТ "Вінницький молочний завод "Рошен" показано на рис. 1.8.

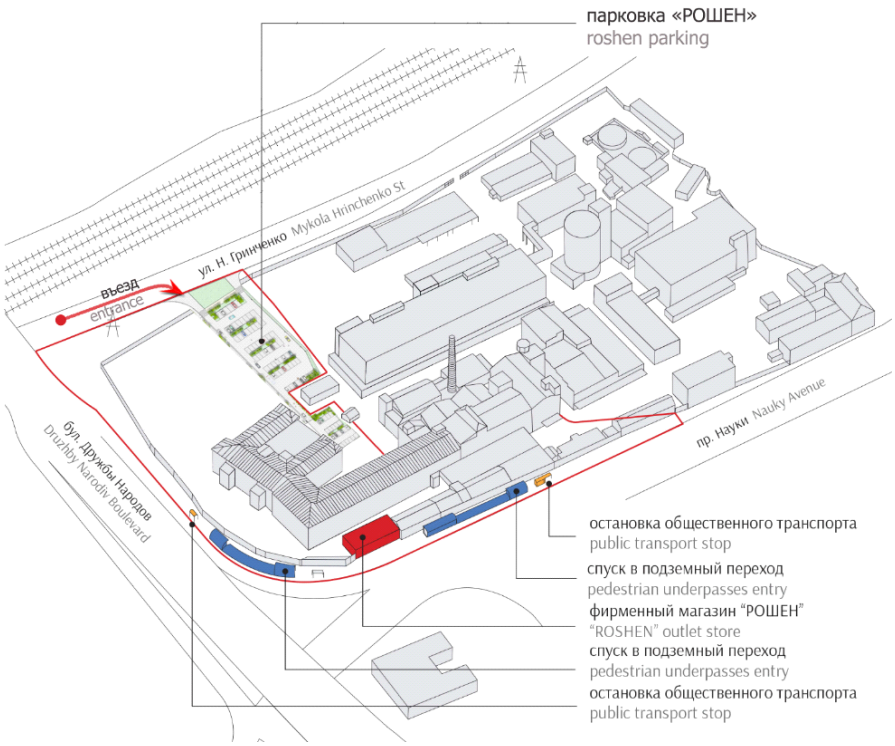


Рисунок 1.8 – План ПРАТ "Вінницький молочний завод "Рошен"

У березні 2016 року «Вінницький молочний завод «Рошен» успішно пройшов аудит та підвищив сертифікацію ISO 22000 до сертифікації FSSC-22000.

Виготовлена продукція регулярно проходить сертифікацію на відповідність вимогам стандартів «Halal» і «Kosher».

З моменту відкриття «Вінницький молочний завод «Рошен» пройшов оцінку та є надійним постачальником молочних продуктів до міжнародних компаній.

На сьогоднішній день продукція заводу експортується в більше ніж 45 країн світу, в основному до країн Європи, Азії, Америки, Океанії та Африки [4].

1.2 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Сьогодні, в епоху великих даних і штучного інтелекту, з новими технологіями, статистика лежить в основі численних рішень і розробок. Позиція статистики в світі зростає, змінюється і сприйняття статистики, вона стає все більш популярною. Численні статистичні процедури засновані на спеціальних методах, підтримуваних інтенсивним комп'ютерним моделюванням, в той час як статистики і математики не завжди знають, стикаються і стикаються з проблемами сучасної статистики. Набагато краще розуміння між статистиками та математиками має важливе значення для розвитку обох цих областей. Актуальним є також питання: як взаємодіяти на найвищому науковому рівні зі світовими фахівцями з медицини, епідеміології та генетики.

Загальний принцип взаємодії добре встановлений: статистика потребує математики, щоб мати міцну базу для своїх методологій, тоді як математика (і теорія ймовірності, теорія випадкових матриць і гармонічний аналіз, зокрема) отримує вигоду від статистики, яка ставить нові важливі проблеми і, як це було в минулому, вони можуть розвиватися в красивих і глибоких математичних теоріях. Співпраця між двома напрямками має вирішальне значення. Для вирішення проблеми слід зібрати статистиків світового класу, які використовують чудову математику, і математиків, які працюють у своїй сфері

інтересів. Слід обговорити останні досягнення сучасної статистики, що вимагають широкого використання глибинних математичних методів і моделей.

Слід зробити акцент на детальному викладі математики, що стоїть за інструментами, що використовуються в статистиці. Важливо якомога точніше описати математичний статус-кво останніх досягнень сучасної статистики і, що ще важливіше, виявити математичні проблеми сучасних статистичних теорій, що відповідають нагальним потребам вибору моделей в медицині, епідеміології та генетиці [7].

Логістичний центр "Рошен" (м. Яготин) на сьогодні забезпечений новітньою системою управління товарними потоками Warehouse Management System.

WMS – це інтелектуальна система, яка не тільки все враховує, але й оптимізує логістичні процеси, що виникають з моменту прийняття і аж до відвантаження товару зі складу. До моменту прибуття автомобіля на склад, документація на його заповнення вже передана, врахована і оброблена. Це дає можливість заздалегідь сформувати замовлення, тому безпосередньо завантаження займає 30-35 хвилин. Таким чином, загальний час перебування вантажного транспорту на території центру не перевищує однієї години [6].

1.3 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань

1.3.1 Мережеве управління підприємством

Історія фірми Digital Enterprise це успішна цифрова трансформація на практиці. Для того щоб стати цифровим підприємством і прискорити свою цифрову трансформацію можна скористатися можливостями програмного продукту Industry 4.0 від Digital Enterprise. Застосування цього значно продукту прискорить цифрову трансформацію для підприємства. За допомогою мережевого програмного комплексу Siemens Xcelerator значно простіше

об'єднати реальний та цифровий світи, щоб збирати, розуміти та осмисллено використовувати згенеровані дані. Нескінченна кількість даних дозволяє ефективно використовувати обмежені ресурси та забезпечувати стійкість і гнучкість виробництва в обраній промисловій галузі.

Індустріальний світ стикається з швидко мінливими викликами, включаючи геополітичну напруженість, технологічні зміни, зрушення на глобальних ринках і вплив зміни клімату. Цифровізація, комп'ютерні системи, мережі даних та автоматизація змінюють правила гри для вирішення цих проблем. Важливо збирати, розуміти та використовувати величезну кількість даних, створених у промисловому Інтернеті речей (ІТОТ). Цифрове підприємство робить саме це, поєднуючи реальний і цифровий світи.

Поєднання реального та цифрового світів дозволяє легко інтегрувати весь ланцюжок створення вартості від проектування до реалізації, оптимізуючи при цьому безперервний потік даних. Справжнє цифрове підприємство здатне використовувати необмежену потужність даних, отримуючи цінну інформацію для прийняття швидких і впевнених рішень, а також створювати найкращі у своєму класі продукти завдяки ефективному виробництву.

Siemens Xcelerator – це перш за все відкрита цифрова бізнес-платформа, яка допомагає швидше впроваджувати інновації і в кінцевому підсумку стати цифровим підприємством. Тоді ви зможете інтегрувати весь життєвий цикл продукту з життєвим циклом фабрики та заводу, а також дані про продуктивність за допомогою нашого комплексного підходу цифрового двійника. Результатом є безперервний відкритий цикл оптимізації, як для продукту, так і для виробництва.

Комплексний підхід цифрового двійника забезпечує безперервну оптимізацію протягом усього життєвого циклу продукту та виробництва, забезпечуючи швидке впровадження продукту, гнучке виробництво та оптимізацію продуктивності на основі даних.

Вивчаючи сценарії «а що, якщо» і прогнозуючи майбутню продуктивність за допомогою цифрового двійника, ви можете бути впевнені, що ваш продукт і виробництво будуть працювати саме так, як ви задумали і запланували.

1.3.2 Способи інтеграції

Горизонтальна інтеграція – безперебійний потік даних по всьому ланцюжку створення вартості в цифровому підприємстві Інтегрований підхід до цифрового підприємства забезпечує горизонтальну інтеграцію та цифровізацію всього ланцюжка створення вартості – від проектування до виробництва, обслуговування та переробки. Безшовна горизонтальна інтеграція усуває прогалини між інформаційними сховищами та пов'язує все, від інновацій продукту до виробництва та використання продукту.

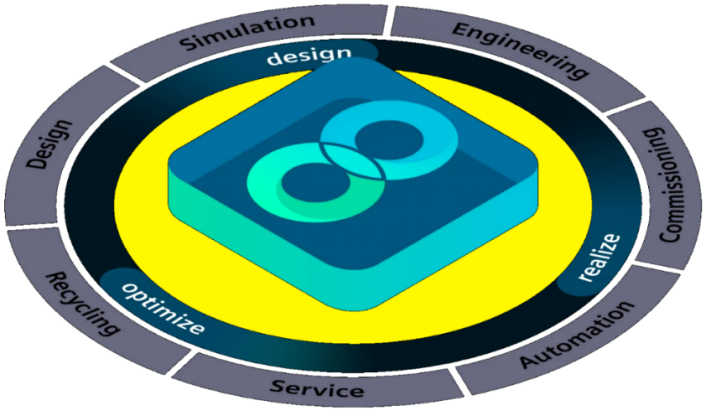


Рисунок 1.9 – Горизонтальна інтеграція

У цифровому підприємстві вертикальна інтеграція з'єднує всі дані від цеху до верхнього поверху Вертикальна інтеграція – конвергенція IT/OT: дані від цеху до верхнього поверху цифрового підприємства.

Усі польові пристрої та блоки управління, що працюють у цеху, виробляють багато даних. Можливості Industry 4.0 залежать від розумного використання даних та комунікації. Вертикальна інтеграція додає саме ці можливості аналізу даних, від інформаційних технологій на верхньому поверсі

також до операційних технологій у цеху – для прийняття рішень на основі даних [5].

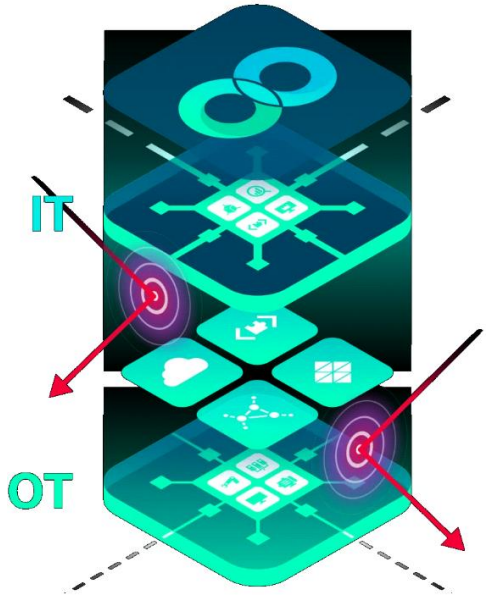


Рисунок 1.10 – Вертикальна інтеграція

1.4 Розробка схеми організаційної структури підприємства

ПРАТ "Вінницький молочний завод "Рошен" має організаційної структуру як частину набору діаграм стратегічного моделювання, що дозволяє моделювати організаційні структури.

Ролі в організаційній діаграмі можуть бути пов'язані з будь-якою кількістю елементів моделі, включаючи заяви про бачення, бізнес-цілі, завдання, процеси та вимоги зацікавлених сторін. Існує також корисний механізм, щоб показати різних людей, які займають ролі з часом, використовуючи екземпляри класів.

Організаційна діаграма бізнес-аналізу входить до групи стратегічного моделювання та відображає структуру організації, яка включає посадових осіб, ролі, обов'язки, підрозділи або відділи. Ролі або підрозділи можна відобразити на схемі за допомогою макета дерева або подання списку. Будь-яку кількість значень з тегами можна додати до елементів або сполучних ліній, щоб додати

додаткову інформацію за потреби. Елементи, з яких складається організаційна діаграма, потім можна використовувати в інших частинах моделі, таких як призначення власників бізнесу бізнес-процесам, бізнес-правилам, системам тощо.

Базові плани схеми організаційної діаграми, це перш за все, засіб для базового планування [8].

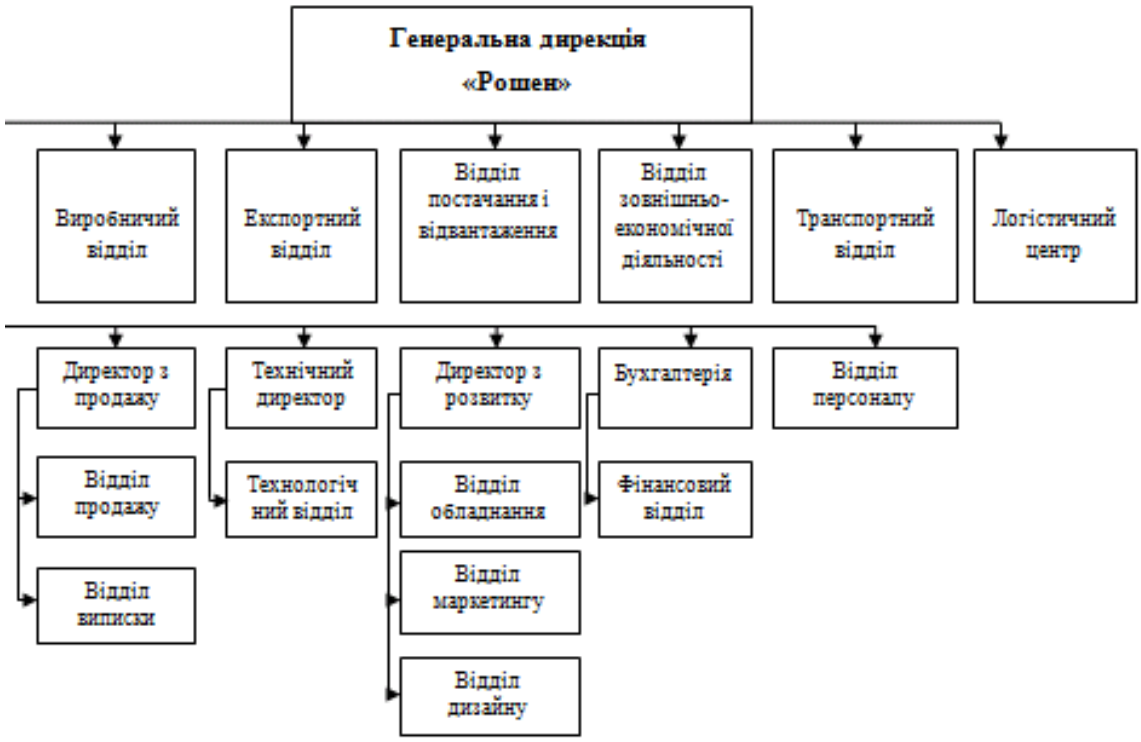


Рисунок 1.11 – Організаційна структура управління ПРАТ "Вінницький молочний завод "Рошен"

Для вдалого використання організаційної структуру слід поєднати команду фахівців ПРАТ "Вінницький молочний завод "Рошен" за допомогою комп’ютерної мережі. Як визначено завданням до кваліфікаційної роботи для синтезу кіберфізичної система з виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі для топологія мережі, яка представлена на рис. 1.13 з наведеними нижче параметрами.

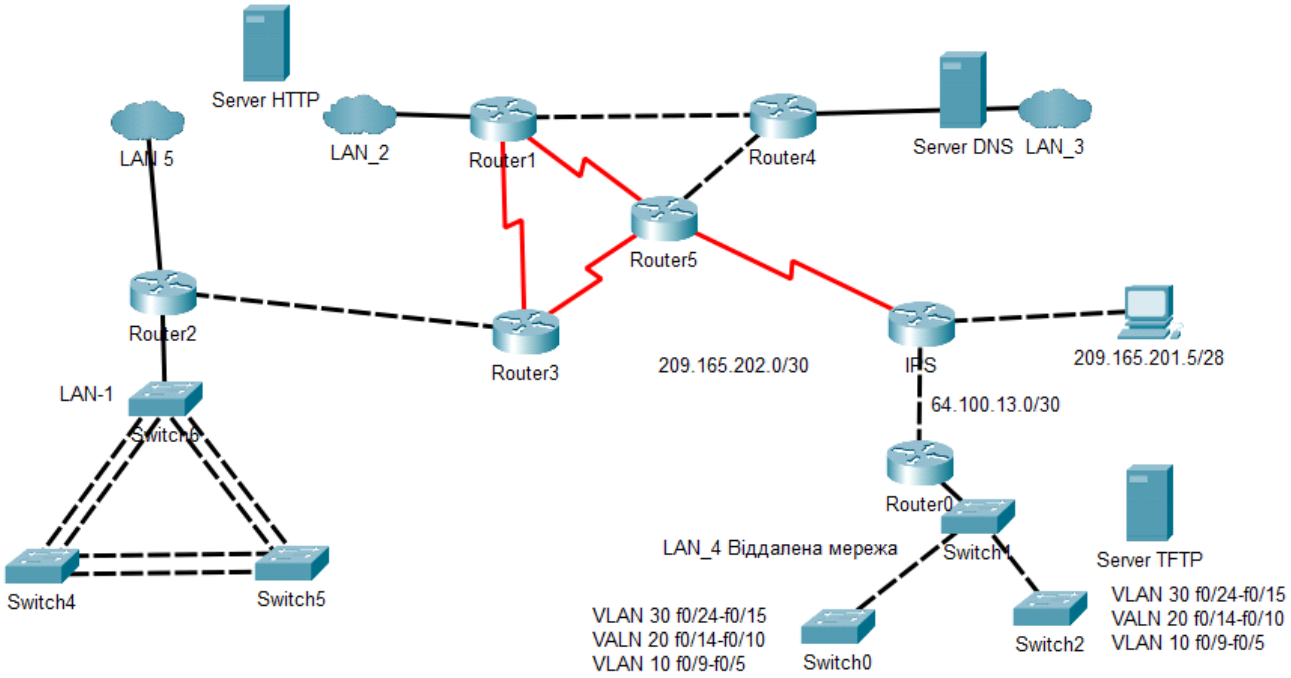


Рисунок 1.12 – Топологія мережі ПРАТ "Вінницький молочний завод "Рошен"

Параметри LAN:

- блок адрес для виділення підмереж: 10.23.IPn.0/22;
- значення IPn блоку адрес виділення підмереж IPn: 16
- кількості вузлів для мережі LAN1: 68;
- кількості вузлів для мережі LAN2, од.: 15;
- кількості вузлів для мережі LAN3, од.: 65;
- кількості вузлів для мережі LAN4, од.: 99;
- кількості вузлів для мережі LAN5, од.: 88;
- інтенсивність найбільшої мережі, μ (кадрів/с): 87.

Розподіл мереж між маршрутизаторами (WAN):

- блок адрес для каналів між маршрутизаторами 10.0.№.0/24;
- номер варіанту № 1;
- перші можливі для використання IP-адреси призначати інтерфейсам і під-інтерфейсам маршрутизаторів у LAN;
- інші з можливих IP-адрес призначати комутаторам у LAN;

- адреса серверів: перший можливий адресу у мережі + 9 + №.
- адреса вузлів: інші з використаних;
- в мережах VLAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

1.5 Постановка завдання

Згідно до кваліфікаційної роботи бакалавра необхідно розробити комп’ютерну систему, яка необхідна для впровадження на ПРАТ "Вінницький молочний завод "Рошен" для управління якістю та безпеки харчових продуктів відповідно до вимог міжнародних стандартів ISO 9001 та ISO 22000. Тобто треба розробити кіберфізична систему контролю за підрозділом з виготовленням вершкового масла з детальним опрацюванням побудови і відповідним налаштування корпоративної мережі.

Враховуючи архітектуру кіберфізичної системи з виготовлення вершкового масла для ПРАТ "Вінницький молочний завод "Рошен", попередньою кількість необхідних підмереж, їх взаємозв’язків та кількості комп’ютерів, необхідно виконати розрахунок налаштувань для заданої топології мережі, здійснити вибір інтерфейсу каналів зв’язку та протоколу обміну, провести розрахунок топологічної схеми комп’ютерної системи, розрахунок налаштувань маршрутизації комп’ютерної мережі, а також виконати подальше моделювання і перевірки роботи комп’ютерної системи.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Розробка структурної схеми підсистеми управління

У кваліфікаційній роботі, в якості об’єкту управління, по завданню керівника, обрано технологічне обладнання з однієї з ліній виготовлення вершкового масла на ПРАТ "Вінницький молочний завод "Рошен" – маслоутворювач ТВФ-2.06.

У маслоутворювачі здійснюється швидке одночасне охолодження і інтенсивне переміщування розтопленої сировини з високим вмістом жиру перетворює її в готовий продукт – масло. Режим роботи маслоутворювача повинен визначатися технологічною картою виготовлення відповідно до моделі пристрою, сезонними змінами хімічного складу молочного жиру, результатами контролю консистенції продукту.

Для нормального режиму роботи маслоутворювача необхідно забезпечити:

- швидке, рівномірне і достатнє охолодження суміші;
- постійну температура суміші жирів на вході в межах 60…70 °С;
- рівномірну подачу суміш жирів до маслоутворювача;
- безперебійну роботу і безперервну продуктивність маслоутворювача протягом усього періоду виробництва;
- постійну циркуляцію холодоагенту в просторі внутрішніх стінок циліндрів.

Перші порції недостатньо охолодженого і переробленого спреду, який виходить з маслоутворювача, повертаються в технологічний процес.

Протягом усього процесу підтримують стабільну роботу маслоутворювача.

Маслоутворювач Тетра Отич ТВФ-2.06 використовується для виробництва всіх видів вершкового масла методом перетворення високо-жирних вершків методом переохолодження, продуктивність установки – 2’000 кг/год (рис. 2.1).

Кожен теплообмінний циліндр маслоутворювача має індивідуальний привід. Приводи, які беруть найбільше навантаження мають ремінну передачу, що дозволяє здійснювати більш інтенсивну механічну обробку продукту. Використовується спеціальний ротор голчастого типу. Він дозволяє поліпшити консистенцію продукту. Це обладнання для виробництва масла дозволяє отримувати продукт, придатний для потокової розфасовки на автоматах типу АРМ.

Маслоутворювач ТВФ-2.06 має пульт автоматики захисту від перевантаження двигунів і відображає навантаження на двигуни циліндрів.

Технічні показники маслоутворювача ТВФ-2.06 представлені в табл. 2.1.

Таблиця 2.1 – Технічні показники маслоутворювача ТВФ-2.06 [9]

№	Назва показників	Значення показників
1	Продуктивність при виробленні, кг / год, не менше	
	вершкового масла селянського чи любительського	2’000
	вершкового масла бутербродного	1’700
	масла традиційного складу	2’000
	масла зниженої жирності	1’700
2	Режим роботи	безперервний
3	Встановлена потужність, не більше, кВт	29
4	Споживання за годину роботи при виробленні масла	
	електроенергії, не більше, кВт	29
	холоду, не більше, кВт	140
5	Габаритні розміри, не більше, мм	
	довжина	1’900
	ширина	1’350
	висота	1’300
6	Маса, не більше, кг	1’454

Рисунок 2.1 – Маслоутворювач Тетра Отич ТВФ-2.06

Система управління маслоутворювачем ТВФ-2.06 має наступні датчики і виконавчі пристрої.

Датчики:

- температура масла на вході, °С 60...70;
- температура масла на виході, °С 15...17;
- температура холодоагенту, °С -8...-3;
- тиск холодоагенту на вході, МПа 3,8...10,7;
- тиск масла в робочих циліндрах на вході, МПа: 0,2...0,5.
- тиск масла в робочих циліндрах на виході, МПа: 2,2...4,1;

Виконавчі пристрої:

- двигун компресора холодоагенту, В /кВт ~380 / ~16,6;
- двигун насосу подачі масла на вході, В /кВт ~380 / ~5,8;
- двигун циліндра-1, В /кВт ~380 / ~1,8;
- двигун циліндра-2, В /кВт ~380 / ~1,8;
- двигун циліндра-3, В /кВт ~380 / ~1,8.

Для економічної роботи маслоутворювача ТВФ-2.06 треба забезпечити регулювання потужності компресору тиску холодоагенту та насосу подачі

масла на вході, тобто забезпечити пропорційний режим їх роботи застосовуючи для управління їх роботою частотні перетворювачі.

Роботою маслоутворювача ТВФ-2.06 управляє програмований логічний контролер – ПЛК (рис. 2.1).

Система управління має підтримувати задану температуру масла на виході в межах встановленого діапазону контролюючі її температуру, контролюючі температуру масла на вході, та за допомогою відповідного регулювання тиску масла на вході, тиску масла на виході, , тиску холодоагенту на вході.

На рис. 2.1 показана структурна схема системи управління маслоутворювачем ТВФ-2.0

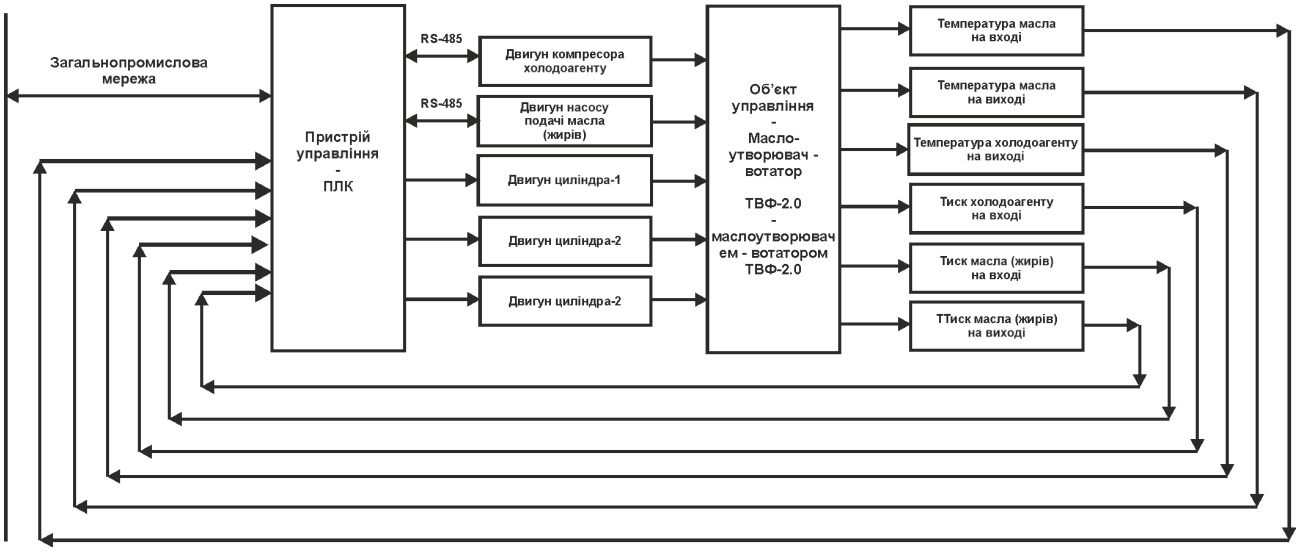


Рисунок 2.1 – Структурна схема підсистеми управління

Датчики забезпечують необхідної первинною інформацією систему управління. Система управління маслоутворювачем ТВФ-2.06 підтримує задану температуру масла на виході межах заданого діапазону температур.

Роботою скребкового маслоутворювача ТВФ-2.06 управляє автоматична система, яка має наступні вихідні сигнали управління:

- двигун компресора холодоагенту пропорційне управління;
- двигун насосу подачі масла (жирів) пропорційне управління;

- двигун циліндру-1 релейне управління;
- двигун циліндру-2 релейне управління;
- двигун циліндру-3 релейне управління.

2.2 Розробка структурної схеми інформаційних потоків

Система управління маслоутворювачем ТВФ-2.06 має пристрої збору інформації (датчики), еталони стану обладнання (технологічна карта процесу виготовлення масла), параметри контролю стану обладнання, програму управління, виконавчі пристрої (електродвигуни).

2.3 Вибір апаратного забезпечення підсистеми управління

2.3.1 Вибір датчиків

Для автоматизації роботи маслоутворювача ТВФ-2.06 необхідно вимірювати температуру масла на вході, масла на виході, температуру холодоагенту на виході - тобто можна мати один тип датчика температури з діапазоном вимірювання –8…70 °С, зі стандартним вихідним струмовим інтерфейсом для підключення до програмованого логічного контролера.

Обрано датчик температури МВТ 3560 (рис. 2.2), який є термоелектричним перетворювачем зі стандартним струмовим сигналом 4…20 мА.

Технічні характеристики датчика наведені в табл. 2.1 [10].

Рисунок 2.2 – Датчик температури MBT 3560

Таблиця 2.1 – Технічні характеристики датчика температури MBT 3560

№	Найменування параметра	Значення
1	Тип	Pt1000
2	Діапазон вимірюваних температур, °С	-50…200
3	Клас допуску	1
4	Точність, °С	±1,5t
5	Діапазон вихідного сигналу, мА	4…20
6	Напруга живлення, В	12…36
7	Потужність споживання, Вт	1

Для вимірювання тиску холодоагенту на вході, тиску масла на вході, тиску масла в робочих циліндрах на виході будемо використовувати датчик тиску серії MBS 1700 з відповідними діапазонами вимірювання (рис. 2.3).

Рисунок 2.3 – Датчик тиску серії MBS 1700

Датчик тиску має відповідно два стандартний вихід 4….20 мА для підключення до програмованого логічного контролера (ПЛК) [11].

Таблиця 2.2 – Технічні параметри датчику тиску серії MBS 1700

№	Найменування параметра	Значення
1	Тип	Комплексне вимірювання
2	Діапазон вимірювання, МПа	0…16
3	Похибка вимірювання, %	±0,5%
4	Частота відгуку, Гц	0,1
5	Напруга живлення, В	12…24
6	Потужність споживання, Вт	4
7	Діапазон температур, °С	-40 до 85
8	Вихідний сигнал, мА	4…20

На підставі обраних датчиків та їх технічних характеристик складена табл. 2.3.

Таблиця 2.3 – Датчики

№	Назва параметру	Принцип дії	Тип	Діапазон змінення	Точність	Значення виходу	Період оновлення	Напруга живлення	Потужність споживання
1	Температура масла на вході	Pt1000	Аналоговий	?50...100° С	±1,5 %	4...20 мА	0.1 с	12…36 В	1 Вт
2	Температура масла на виході	Pt1000	Аналоговий	?50...100° С	±1,5 %	4...20 мА	0.1 с	12…36 В	1 Вт
3	Температура холодоагенту на виході	Pt1000	Аналоговий	?50...100° С	±1,5 %	4...20 мА	0,1 с	12…36 В	1 Вт
4	Тиск холодоагенту на вході	Тензо	Аналоговий	0…16 МПа	±0,5 %	4...20 мА	0.1 с	12…24 В	5 Вт
5	Тиск масла на вході	Тензо	Аналоговий	0…5 МПа	±0.5 %	4...20 мА	0,1 с	12…24 В	4 Вт
6	Тиск масла в робочих циліндрах на виході	Тензо	Аналоговий	0…0,5 МПа	±0.5 %	4...20 мА	0,1 с	12…24 В	4 Вт

2.3.2 Вибір виконавчих пристроїв

В системі управління мають бути вихідні ланцюг узгодження з наступним технологічним електрообладнанням:

- двигун компресора холодоагенту;
- двигун насосу масла на вході;
- двигун циліндра-1;
- двигун циліндра-2;
- двигун циліндра-3.

Для приводу компресору холодоагенту використовується асинхронний трьох фазний електропривод потужністю 16,6 кВт. Згідно з завданням система управління повинна реалізовувати плавне регулювання продуктивності подачі тику. Таким чином управління має бути пропорційним. Таким чином для управління електроприводом обрано трьох фазний частотний перетворювач GD20-022G-4 (22 кВт) з інформаційним входом управління RS-485 (рис. 2.4) [12].

Технічні характеристики частотного перетворювача наведені в табл. 2.4.

Рисунок 2.4 – Частотний перетворювач GD20-022G-4

Таблиця 2.4 – Технічні характеристики частотного перетворювача GD20-022G-4

Найменування параметра	Значення
Тип	Скалярний
Напруга живлення, В	~320…~550
Потужність, кВт	22,0
Діапазон частот, Гц	0…240
Канал управління	RS-485 (MODBUS)
Ступінь захисту	IP20

Для приводу насосу подачі масла на вході використовується асинхронний трьох фазний електропривод потужністю 5,8 кВт. Згідно з завданням система управління повинна реалізовувати пропорційне управління. Таким чином для управління електроприводом обрано трьох фазний частотний перетворювач GD200A-011G/015P-4 (11,0 кВт(з аналоговим входом 4…20 мА (рис. 2.5) [12].

Технічні характеристики частотного перетворювача наведені в табл. 2.5.

Рисунок 2.6 – Частотний перетворювач GD200A-011G/015P-4

Таблиця 2.5 – Технічні характеристики частотного перетворювача GD200A-011G/015P-4

Найменування параметра	Значення
Тип	Скалярний
Напруга живлення, В	~320…~550
Потужність, кВт	22,0
Діапазон частот, Гц	0…240
Канал управління	RS-485 (MODBUS)
Ступінь захисту	IP20

Трифазні двигуни циліндрів, потужністю 2 кВт кожний, мають дискретний тип управління.

Рисунок 2.7 – Трифазне твердотільне реле TRT-60LA SSR (3x~380 В, 4…20 мА)

Тому для їх управління використаємо трифазне твердотільне реле змінного струму TRT-60LA SSR з каналом керування 4…20 мА, яке будемо використовувати у дискретному режимі управління [12].

Таблиця 2.6 – Технічні характеристики трифазного твердотільне реле TRT-60LA SSR

Найменування параметра	Значення
Тип	NBR
Напруга навантаження, В	~600 В
Струм навантаження, А	0…60
Струм управління, мА	4…20

На підставі наведеного вище для виконавчих пристроїв, та їх технічних характеристик складена табл. 2.7.

Таблиця 2.7 – Виконавчих пристроїв

№	Назва параметру	Принцип дії	Тип	Діапазон змінення	Лінійність	Значення входу	Період оновлення	Напруга живлення	Потужність споживання
1	Тиск компресора холодоагенту	RS-485 (MODBUS)	Аналоговий	0…16 МПа	Лінійній	-	115 кбод/с	-	-
2	Насос подачі масла на вході	RS-485 (MODBUS)	Аналоговий	00…5 МПа	Лінійній	-	115 кбод/с	-	-
3	Ціліндр-1	Твердотільне реле	Дискретний	вимк./вкл..	Не лінійний	4…20 мА	0,1 с	24 В	1,0 Вт
4	Ціліндр-1	Твердотільне реле	Дискретний	вимк./вкл..	Не лінійний	4…20 мА	0,1 с	24 В	1,0 Вт
5	Ціліндр-1	Твердотільне реле	Дискретний	вимк./вкл..	Не лінійний	4…20 мА	0,1 с	24 В	1,0 Вт

2.3.3 Вибір пристроїв управління

Відповідно вимогам до підсистеми управління, що розробляється, в якості пристрою управління використовується ПЛК компанії VIPA.

Контролер має модульну структуру, що забезпечуєь підключення тільки обраного периферійного обладнання, та забезпечить легке розширення подальшого функціоналу.

До контролеру повинні бути підключені шість датчиків, які мають уніфікований стандартний тип виходу 4...20 мА.

До контролеру повинні бути підключено три канали дискретного управління (тип виходу 4, 20 мА) для управління трьома трифазними двигунами перемішувачів масла у циліндрвх.

Два трьох фазні частотні перетворювач допомогою інформаційного каналу RS-485 управляють продуктивністю виконавчих пристроїв.

Так як система управління маслоутворювачем має інтегруватися у загально-заводську автоматизовану систему управління АСУ ТП, то вона повинна мати стандартний послідовний канал зв’язку, визначений раніше – RS-485 з протоколом MOLBUS, або мережевий канал Ethernet.

Наведеним вимогам відповідає програмований логічний контролер VIPA 214-2BS33 (рис. 2.7), технічні характеристики якого наведені в табл. 2.8.

Рисунок 2.7 – Програмований логічний контролер VIPA 214-2BS33

Таблиця 2.8 – Технічні характеристики програмованого логічного контролеру VIPA 214-2BS33

№	Найменування параметра	Значення
1	Тип	CPU 214SER
2	Пам’ять, кбайт	144
3	Робоча пам’ять, кбайт	96
4	Максимальна кількість модулів, штук	32
5	Час виконання команди над бітом, мкс	0,18
6	Час виконання команди над байтом, мкс	0,78
7	Час виконання команди над словом, мкс	1,8
8	Час виконання команди над двійним словом, мкс	40,0
9	RS-485 інтерфейс	Присутній
10	Напруга живлення, В	24
11	Споживана потужність, Вт	5

Для підключення усіх шести датчиків , які мають стандартний струмовий сигнал 4...20 мА, обрано два модулі аналогового вводу VIPA 231-1BD40, кожних з яких який має по чотири аналогові входи (рис. 2.8), технічні характеристики якого наведені в табл. 2.9.

Рисунок 2.8 – Модуль аналогового вводу VIPA 231-1BD40

Таблиця 2.9 – Технічні характеристики модуля аналогового вводу VIPA 231-1BD40

№	Найменування параметра	Значення
1	Тип	SM 231, ECO
2	Кількість каналів	4
3	Тип каналу	Аналоговий
4	Діапазон вхідного сигналу, мА	4...20
5	Довжина екранованого провідника, м	200
6	Споживана потужність, Вт	0.6

До контролеру повинно бути підключено три дискретні канали управління (тип виходу 4, 20 мА), тому обрано модуль аналогового виводу з діапазоном аналогового сигналу 4…20 мА VIPA 232-1BD40 який має чотири аналогових виходи 4…20 мА (рис. 2.9). Технічні характеристики модулю наведені в табл. 2.10.

Рисунок 2.9 – Модуль аналогового виводу VIPA 232-1BD40

Таблиця 2.10 – Технічні характеристики модуля аналогового виводу VIPA 232-1BD40

Найменування параметра	Значення
Тип	SM 232, ECO
Кількість каналів	4
Тип каналу	аналоговий
Діапазон вхідного сигналу, мА	4…20, -20…+20
Довжина екранованого провідника, м	200
Споживана потужність, Вт	1,5

Згідно з вимогами до підсистеми управління, в якості котрого виступає програмований логічний контролер, та пультом оператора, в якості якого виступає персональний комп’ютер, повинна бути організована мережа за допомогою інтерфейсу RS-485. Обраний програмований логічний контролер VIPA 214-2BS33 має інтерфейс RS-485. Схема підключення персонального комп’ютеру до програмованого логічного контролеру наведена на рисунку 2.13.

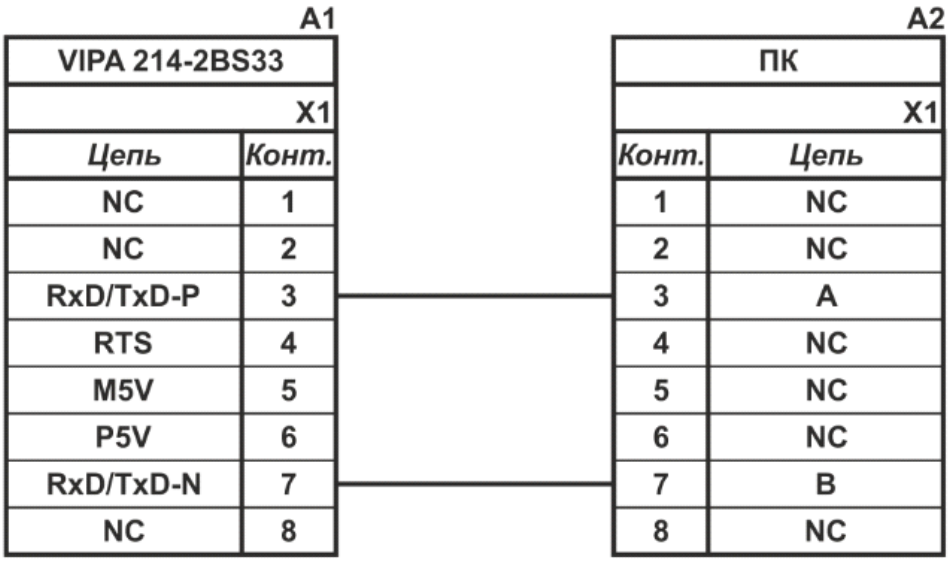


Рисунок 2.10 – Схема підключення по інтерфейсу RS-485

На підставі обраного програмованого логічного контролера та його модулів складена табл. 2.11.

Таблиця 2.11 – Пристрій управління та його модулі

№	Назва модуля	Пристрій	Живлення	Потужність
1	VIPA 214-2BS33	**Центральний процесорний модуль**	**24 В**	**5.00 Вт**
		Зв'язок - АСК ТП		
2	VIPA 231-1BD40	**Модуль аналогового вводу**	**24 В**	**0.60 Вт**
		Температура масла на вході	24 В	1.00 Вт
		Температура масла на виході	24 В	1.00 Вт
		Температура холодоагенту на виході	24 В	1.00 Вт
3	VIPA 231-1BD40	**Модуль аналогового вводу**	**24 В**	**0.60 Вт**
		Тиск холодоагенту на вході	24 В	1.00 Вт
		Тиск масла в робочих циліндрах на вході	24 В	1.00 Вт
		Тиск масла в робочих циліндрах на виході	24 В	1.00 Вт
4	VIPA 231-1BD40	**Модуль аналогового виводу**	**24 В**	**2.00 Вт**
		Циліндр-1	24 В	1.0 Вт
		Циліндр-2	24 В	1.0 Вт
		Циліндр-3	24 В	1.0 Вт

2.3.4 Вибір джерел живлення

ПЛК та його модулі мають напругу живлення +24 В. Загальна потужність споживання програмованого логічного контролера та його модулів:

	(2.1)

Виходячи з потужності споживання ПЛК та його модулів у якості джерела живлення обрано блок живлення SPD24301 з вихідною напругою +24 В та потужністю 30 Вт (рис. 2.11). Технічні характеристики блока живлення наведені в табл. 2.12.

Рисунок 2.11 – Блок живлення Carlo Gavazzi SPD24301

Таблиця 2.12 – Технічні характеристики блока живлення Carlo Gavazzi SPD24301

Виконавши аналіз обраного обладнання можливо зробити вивід, що зовнішній блок живлення потрібен для датчиків 6: температури, диференційного тису, витратоміру та чотирьох трифазних твердотільних реле, які мають напругу живлення +24 В та потужність споживання:

	(2.2)

Виходячи з потужності споживання датчиків та виконавчого пристрою у якості джерела живлення обрано блок живлення такий самий як і для живлення ПЛК SPD24301 з вихідною напругою +24 В та потужністю 30 Вт.

№	Найменування параметра	Значення
1	Напруга живлення, В	~85...~264
2	Вихідна напруга, В	24
3	Потужність, Вт	30
4	Максимальний вихідний струм, А	1,25

2.4 Розробка функціональної схеми автоматизації

Виходячи з вимог системи управління технологічним обладнанням – маслоутворювачем Тетра Отич ТВФ-2.06 розроблена функціональна схема автоматизації, яка наведена на рис. 2.12.

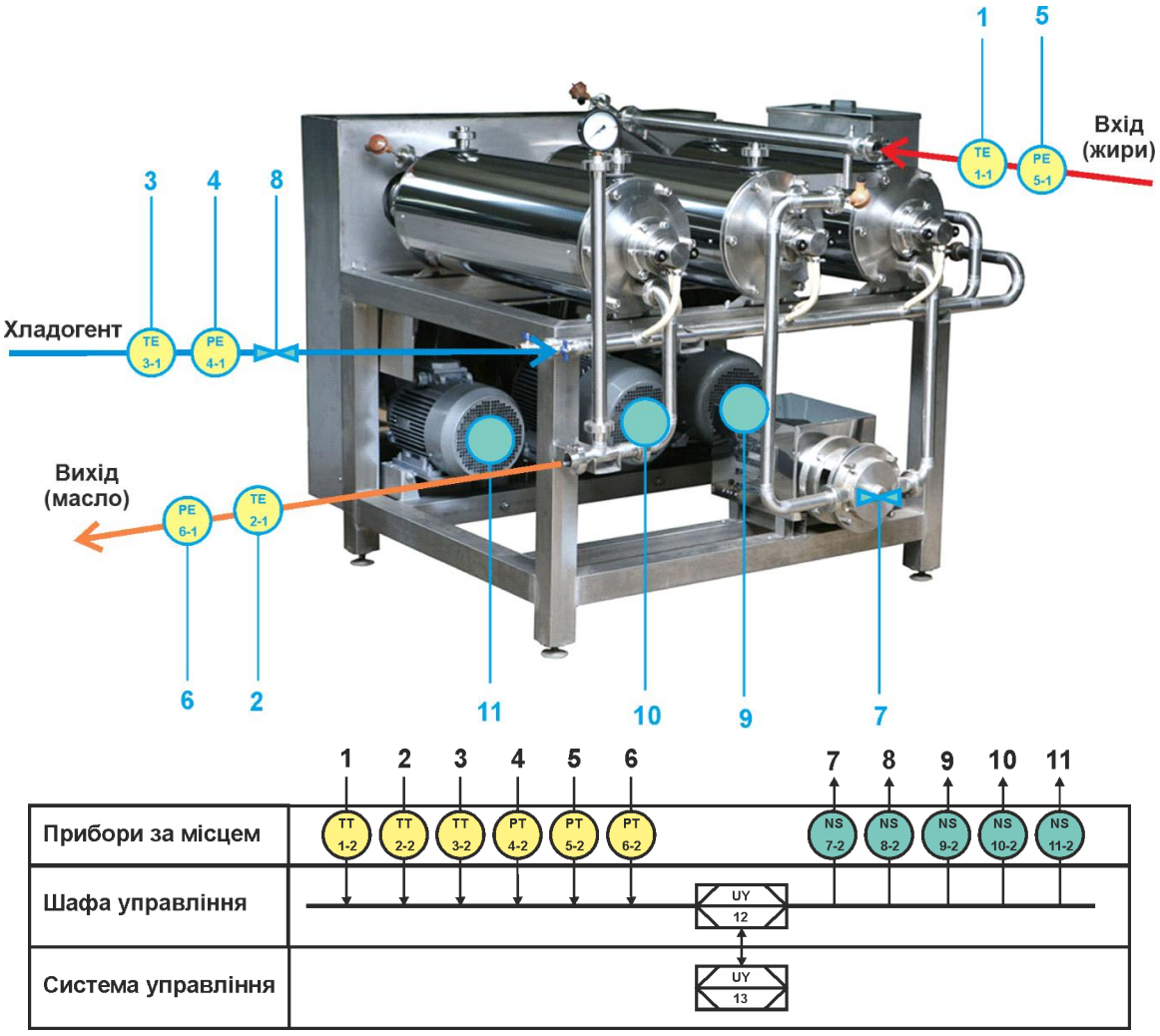


Рисунок 2.12 – Функціональна схема автоматизації маслоутворювачем ТВФ-2.06

У якості пристрою управління використовується ПЛК (UY 12) – VIPA 214-2BS33. Програмований логічний контролер підключено до технологічного обладнання АСУ ТП, за що відповідає система автоматизації більш високого рівня (UY 11), зв'язок між ними реалізовано за допомогою інтерфейсу RS-485.

Для вимірювання трьох параметрів температури: масла на вході (ТЕ 1-1, – МВТ 3560) та перетворювачів 4…20 мА (ТТ 2-1 – МВТ 3560), масла на виході (ТЕ 2-1, – МВТ 3560) та перетворювачів 4…20 мА (ТТ 2-2 - МВТ 3560) та

холодоагенту на виході (ТЕ 3-1 – МВТ 3560) та перетворювачів 4…20 мА (ТТ 3-2 – МВТ 3560).

Для вимірювання трьох параметрів тиску використовуються датчики: тиску холодоагенту на вході (РЕ 4.1 – МВТ 3560) та перетворювачів 4…20 мА (РТ 4.2 – МВТ 3560), тиску масла в на вході РЕ 5.1 – МВТ 3560) та перетворювачів 4…20 мА (РТ 5.2 – МВТ 3560) та тиску масла на виході РЕ 6.1 – МВТ 3560) та перетворювачів 4…20 мА (РТ 6.2 – МВТ 3560).

На підставі отриманих первинних значень від відповідних датчиків програмований логічний контролер (UY 12 – VIPA 214-2BS33) формує керуючі впливи по підтримці заданого температурного режиму маслоутворювача ТВФ-2.06.

Для управління продуктивністю компресору холодоагенту використовується трьох-фазний частотний перетворювач (NS-7 GD20-022G-4) з каналом зв’язку та RS-485.

Для управління продуктивністю насоса подачі масла на вході використовується трьох-фазний частотний перетворювач (NS-8 GD200A-011G/015P-4) з каналом зв’язку та RS-485.

Для управління перемішувачами цилиндру-1…цилиндру-3 використовуються твердотільні реле (NS-9…NS-TRT-60LA SSR) з каналом управління 4…20 мА (використовується релейний режим управління).

2.5 Розробка схеми електричної принципової

На основі функціональної схеми автоматизації та обраного апаратного забезпечення розроблена схема електрична принципова системи управління маслоутворювачем Тетра Отич ТВФ-2.06 (рис. 2.13).

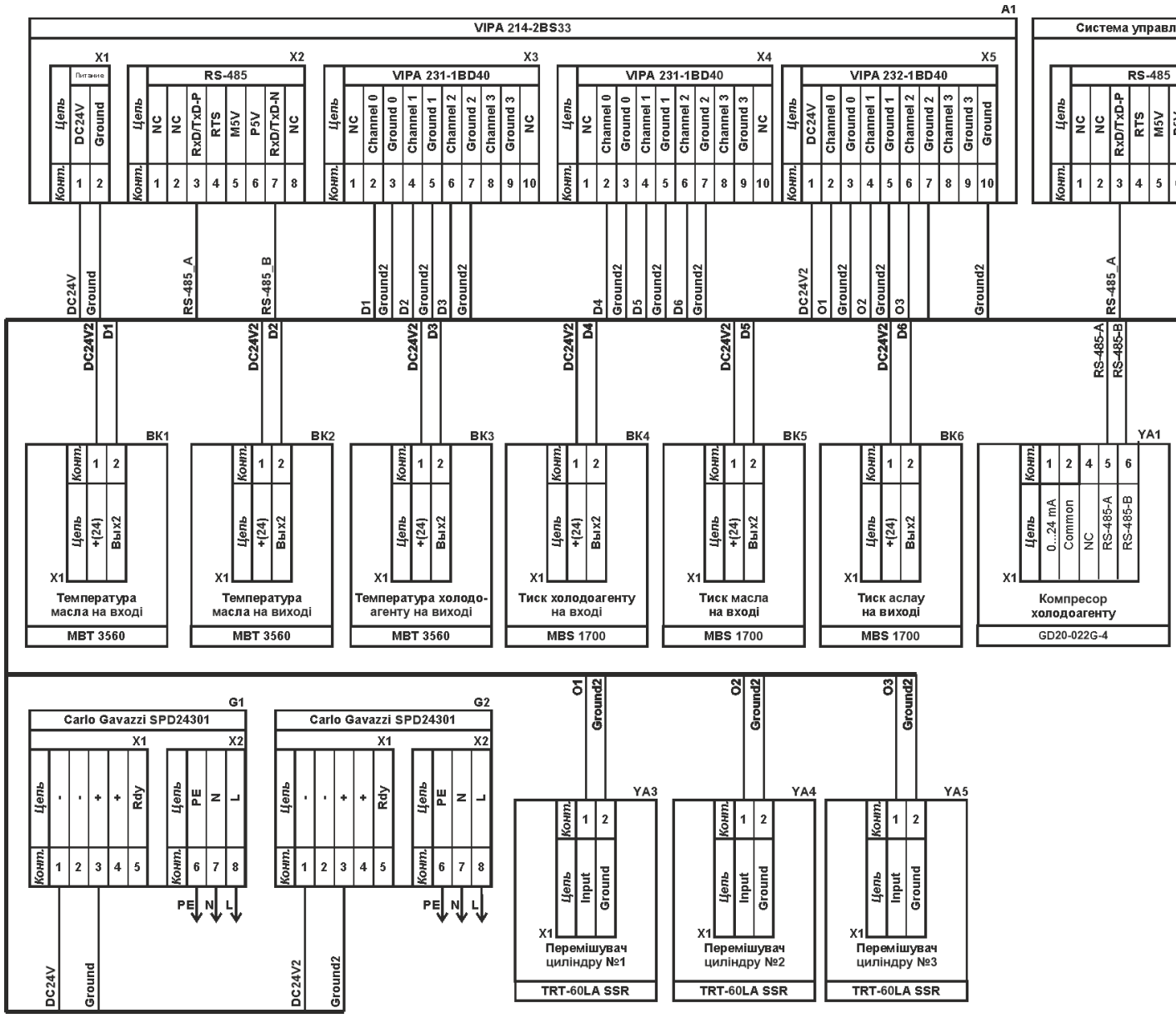


Рисунок 2.13 – Схема електрична принципова системи управління маслоутворювачем Тетра Отич ТВФ-2.06

В підсистемі використовуються два блока живлення. Блок живлення Carlo Gavazzi SPD24301 (G1) підключено до програмованого логічного контролеру VIPA 214-2BS33 (A1). Блок живлення Carlo Gavazzi SPD24301 (G2) підключено до модулю дискретного виводу VIPA 222-1BF00 (A1 – X5), к датчикам температури масла на вході маслоутворювача (ВК1), температури масла на вході маслоутворювача (ВК2), температури масла на виході маслоутворювача

(ВК3), тиску холодоагенту на вході маслоутворювача (ВК4), тиску масла на вході маслоутворювача (ВК5) та тиску масла на виході маслоутворювача (ВК6).

Усі шість аналогових датчиків підключені до двох модулів аналогового вводу VIPA 231-1BD53 (A1 – X3) до каналів 0, 1, 2 та (A1 – X4) до каналів 0, 1, 2, допомогою стандартного сигналу 4…20 мА.

Управління продуктивністю компресора холодоагенту використовується за допомогою трьох-фазного частотного перетворювача YA1 по каналу RS-485.Управління продуктивністю насосу подачі масла на вході маслоутворювача використовується за допомогою трьох-фазного частотного перетворювача YA2 по каналу RS-485.

Управління електродвигунами перемішувачів для циліндру-1…циліндру-3 здійснюється через модуль аналогового виводу VIPA 222-1BF00 (A1 – X5) через ланцюжки O1…O3 (YA3…YA5) – керування здійснюється в релейному режимі. При наявності струму управління 20 мА вони підключають відповідні пристрої управління до трифазної мережи ~380 В, а при сигналі 4 мА вони повертається до виключеного стану.

Зв’язок між програмованим логічним контролером VIPA 214-2BS33 (A1) та АСК ТП верхнього рівня (A2) реалізовано за допомогою інтерфейсу RS-485 (A1 – X2).

2.6 Висновки за розділом

У якості об’єкта управління виступає технологічне обладнання маслоутворювачем Тетра Отич ТВФ-2.06 .

У цьому розділі вибрано апаратно-програмні засоби для створення підсистеми, розроблена функціональна схема автоматизації, розроблена схема принципова підсистеми управління, складено перелік елементів до схеми електричної принципової.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Згідно з завданням до виконання кіберфізичної системи виготовлення вершкового масла для Вінницького молочного заводу «Рошен» використано адресний простір 10.23.16.0/22, а для адресації каналів між маршрутизаторами застосований блок адрес 10.0.1.0/24, перші можливі для використання IP-адреси призначені інтерфейсам і підінтерфейсам маршрутизаторів у LAN, інші з можливих IP-адрес призначені комутаторам у LAN, серверам привласнені IP-адреса за правилом перший можливий адрес у мережі плюс 10.

Розподіл IP-адрес виконано згідно до даних, наведених табл. 3.1, інтенсивність трафіку найбільшої мережі μ =87 кадрів/с.

Таблиця 3.1 – Кількість вузлів в підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
68	15;	65	99	88

Маскування підмережі змінної довжини (VLSM) є більш ефективним способом розподілу мережі. на підмережі Коли виконується класичний розподіл на підмережі, всі підмережі повинні використовувати однакову маску підмережі, змушуючи для всіх підмереж використовувати однакову кількість хостів. Це може призвести до втрати простору IP.

VLSM дозволяє використовувати різні маски підмереж, дозволяючи використовувати більш точну кількість хостів в кожній підмережі.

Використовуючи VLSM калькулятор можна швидко з'ясувати, як найбільш ефективно налаштувати вашу мережу.

Результат розрахунку для мережа 10.23.0.0/22 показую що максимальна кількість 1022 хостів, а для нашого варіанту підмережі потрібно лише 335 хостів.

Результат розподілу підмереж LAN1…LAN5 представлено в табл. 3.1.

Розрахуємо адресацію каналами між маршрутизаторами з застосуванням заданого блоку адрес 10.0.1.0/24.

Враховуючі максимальну кількість вузлів в підмережі WAN, яка дорівнює. 2, можна застосувати блок адрес 10.0.1.0/30.

Визначення підмереж між маршрутизаторами наведено на рис. 3.1.

Результат розподілу підмереж WAN1…WAN5 представлено в табл. 3.3.

Мережа 10.0.1.0/30 має 2 хоста, для WAN підмережам потрібно 10 хостів.

Розрахуємо адресацію в підмережі VLAN застосуванням заданого блоку адрес 10.23.0.0/25.

Результат розподілу для 4 підмереж WLAN20, WLAN30, WLAN40 та WLAN50 представлено в табл. 3.3.

Мережа 10.23.0.0/25 має обмеження у 126 хостів, для WLAN підмереж потрібно 109 хостів.

Схема адресації пристроїв мережі наведена в табл. 3.5.

Таблиця 3.1 – Розподіл адресів для підмереж LAN1…LAN5

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast	Wildcard
LAN1	68	126	58	10.23.1.0	/25	255.255.255.128	10.23.1.1 - 10.23.1.126	10.23.1.127	0.0.0.127
LAN2	15	30	15	10.23.2.0	/27	255.255.255.224	10.23.2.1 - 10.23.2.30	10.23.2.31	0.0.0.31
LAN3	65	126	61	10.23.1.128	/25	255.255.255.128	10.23.1.129 - 10.23.1.2	10.23.1.255	0.0.0.127

							54		
LAN4	99	126	27	10.23.0.0	/25	255.255.255.128	10.23.0.1 - 10.23.0.126	10.23.0.127	0.0.0.127
LAN5	88	126	38	10.23.0.128	/25	255.255.255.128	10.23.0.129 - 10.23.0.254	10.23.0.255	0.0.0.127

Таблиця 3.2 – Розподіл адресів для підмереж WAN1…WAN5

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast	Wildcard
WAN1	2	2	0	10.0.1.0	/30	255.255.255.252	10.0.1.1 - 10.0.1.2	10.0.1.3	0.0.0.3
WAN2	2	2	0	10.0.1.4	/30	255.255.255.252	10.0.1.5 - 10.0.1.6	10.0.1.7	0.0.0.3
WAN3	2	2	0	10.0.1.8	/30	255.255.255.252	10.0.1.9 - 10.0.1.10	10.0.1.11	0.0.0.3
WAN4	2	2	0	10.0.1.12	/30	255.255.255.252	10.0.1.13 - 10.0.1.14	10.0.1.15	0.0.0.3
WAN5	2	2	0	10.0.1.16	/30	255.255.255.252	10.0.1.17 - 10.0.1.18	10.0.1.19	0.0.0.3
WAN6	2	2	0	10.0.1.20	/30	255.255.255.252	10.0.1.21 - 10.0.1.22	10.0.1.23	0.0.0.3

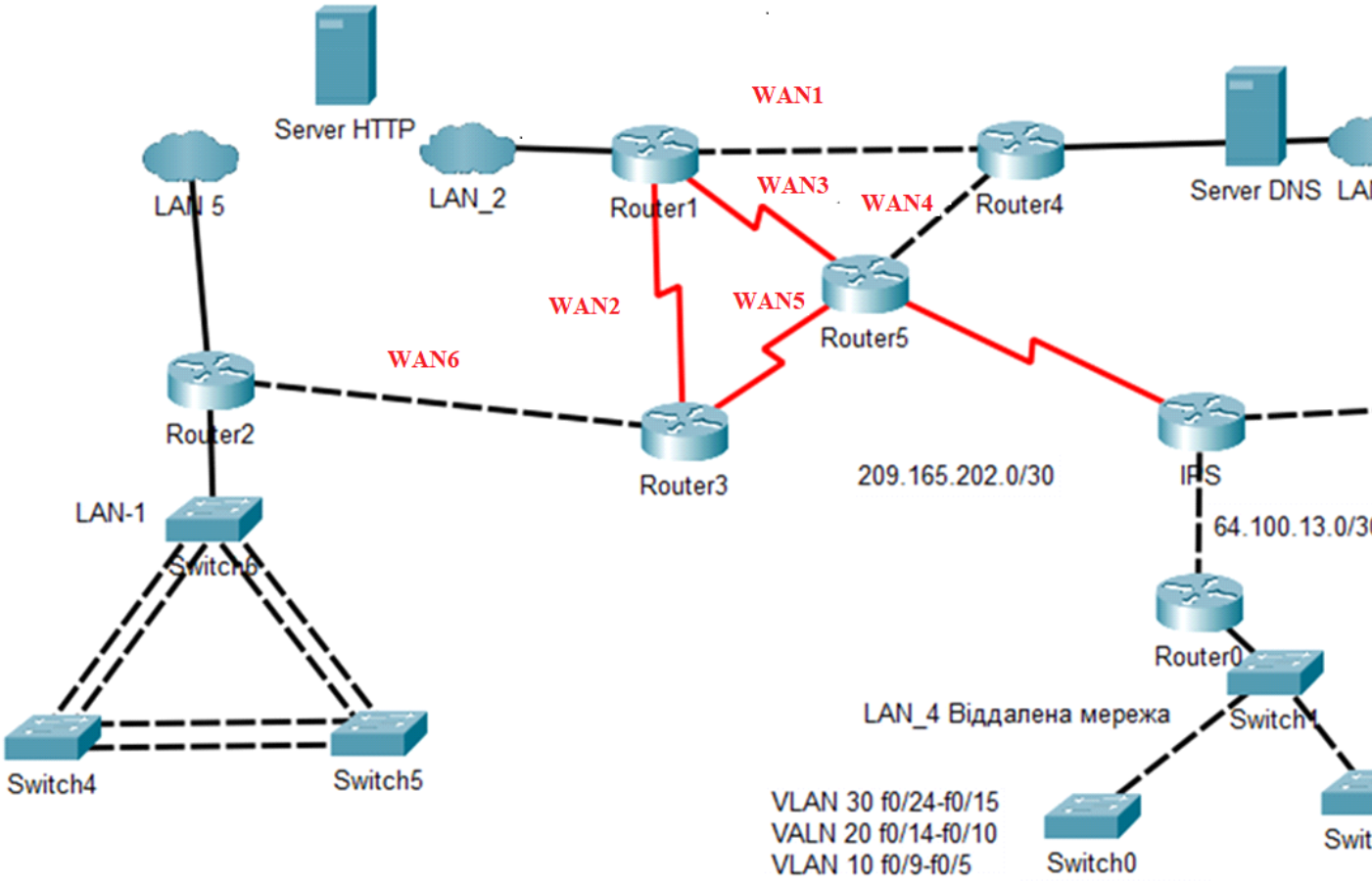


Рисунок 3.1 – Визначення підмереж між маршрутизаторами

Таблиця 3.3 – Схема адресації підмережі мережі VLAN

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
VLAN50	29	30	1	10.23.0.0	/27	255.255.255.224	10.23.0.1 - 10.23.0.30	10.23.0.31
VLAN60	28	30	2	10.23.0.32	/27	255.255.255.224	10.23.0.33 - 10.23.0.62	10.23.0.63
VLAN40	27	30	3	10.23.0.64	/27	255.255.255.224	10.23.0.65 - 10.23.0.94	10.23.0.95
VLAN5	25	30	5	10.23.0.	/27	255.255.255.2	10.23.0.9	10.23.0.1

0				96		24	7 - 10.23.0.126	27

Таблиця 3.4 – Схема адресації підмережі мережі VLAN

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
IPS	2	2	0	209.165.202.0	/30	255.255.255.252	209.165.202.1 - 209.165.202.2	209.165.202.3
Remout1	10	14	4	209.165.201.0	/28	255.255.255.240	209.165.201.1 - 209.165.201.14	Remout1
Remout2	6	6	0	209.165.201.16	/29	255.255.255.248	209.165.201.17 - 209.165.201.22	209.165.201.23

Таблиця 3.5 – Схема адресації пристроїв мережі

Ім'я пристрою	**Інтерфейс**	**IP-адреса**	**Маска**	**Шлюз**
Маршрутизатори				
R1_Anikeev	Fa0/0	10.23.0.128	/25	–
R1_Anikeev	Fa0/1	10.23.1.0	/25	–
R1_Anikeev	Se0/1/1	10.0.1.21	/30	–
R2_Anikeev	Se0/3/0	10.0.1.22	/30	–
R2_Anikeev	Se0/1/1	10.0.1.6	/30	–
R2_Anikeev	Se0/1/0	10.0.1.18	/30	–
R3_Anikeev	Se0/3/0	10.0.1.10	/30	–
R3_Anikeev	Se0/1/1	10.0.1.1	/30	–
R3_Anikeev	Se0/1/0	10.0.1.6	/30	–
R3_Anikeev	Fa0/0	10.23.2.1	/25	–
Router_IPS	Se0/3/1	10.0.1.10	/30	–
Router_IPS	Se0/1/1	10.0.1.17	/30	–
Router_IPS	Se0/3/0	10.0.1.13	/30	–
Router_IPS	Se0/1/1	209.165.202.1	/30	–
R5_Anikeev	Se0/3/1	10.0.1.14	/30	–
R5_Anikeev	Se0/1/0	10.0.1.12	/30	–
R5_Anikeev	Fa0/0	10.23.1.29	/25	–
R6_Anikeev	Se0/1/0	64.100.13.1	/30	–
R6_Anikeev	Fa0/0	10.23.0.1	/25	–

RIPS_Anikeev	Se0/3/1	10.0.1.14	/30	–
RIPS_Anikeev	Se0/1/0	209.165.202.1	/30	–
RIPS_Anikeev	Fa0/0	255.255.255.1	/28	–
LAN1				
LAN_1_PC_1	NIC	10.23.1.1	/25	10.23.1.0
LAN_1_PC_2	NIC	10.23.1.2	/25	10.23.1.0
LAN_1_PC_3	NIC	10.23.1.3	/25	10.23.1.0
LAN_1_PC_4	NIC	10.23.1.3	/25	10.23.1.0
LAN2				
LAN_2_PC_1	NIC	10.23.2.1	/27	10.23.2.0
LAN_2_PC_2	NIC	10.23.2.2	/27	10.23.2.0
LAN_2_PC_3	NIC	10.23.2.3	/27	10.23.2.0
LAN3				
LAN_3_PC_1	NIC	10.23.1.129	/25	10.23.1.128
LAN_3_PC_2	NIC	10.23.1.130	/25	10.23.2.0
Server DNS LAN_3	NIC	10.23.1.131	/25	10.23.2.0
LAN4				
PC_VLAN_1	NIC	10.23.0.1	/25	10.23.0.0
PC_VLAN_2	NIC	10.23.0.2	/25	10.23.0.0
PC_VLAN_3	NIC	10.23.0.3	/25	10.23.0.0
PC_VLAN_4	NIC	10.23.0.4	/25	10.23.0.0
PC_VLAN_5	NIC	10.23.0.5	/25	10.23.0.0
PC_VLAN_6	NIC	10.23.0.6	/25	10.23.0.0
Кінець таблиці 3.3				
LAN5				
LAN_5_PC_1	NIC	10.23.0.129	/25	10.23.0.128
LAN_5_PC_2	NIC	10.23.0.130	/25	10.23.0.128
LAN_5_Server_HTTP	NIC	10.23.0.131	/25	10.23.0.128
Provider				
PC-PT	NIC	209.165.201.5	/28	209.165.201.0

3.2 Розробка топологічної схеми корпоративної мережі

Розроблена топологічна схема Кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен», представлена на рис. 3.1.

.

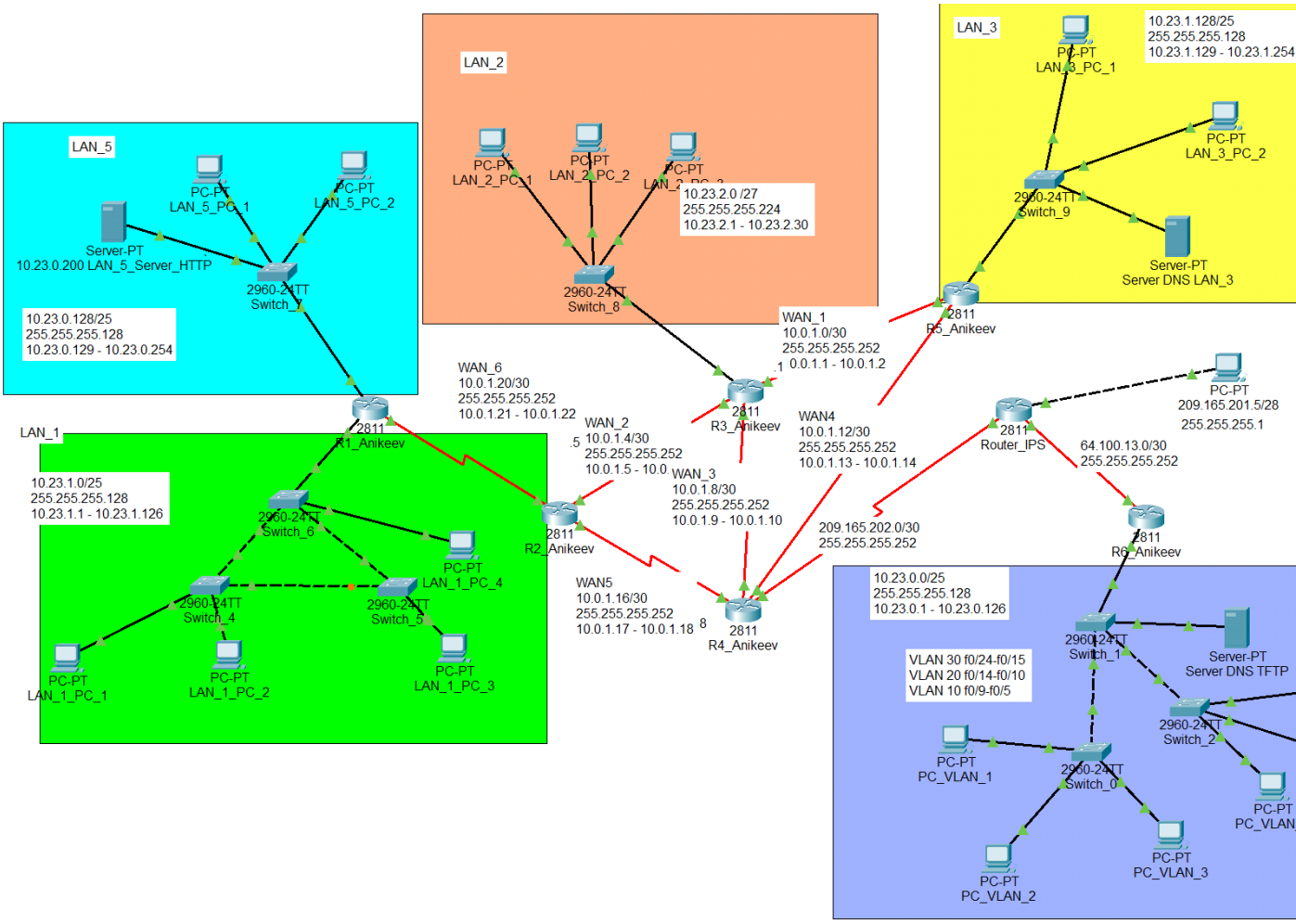


Рисунок 3.2 – Синтезована мережа Вінницького молочного заводу «Рошен»

3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Розроблена топологічна схема кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» застосовує протокол динамічної маршрутизації OSPF, який є дистанційно-векторним протоколом, з номером автономної системи 23.

При налаштуванні маршрутизації на роутерах даної КС, на serial-інтерфейсах, відповідно до технічних умов, встановлено пропускну спроможність 128 кб/с , вартість метрики 7’500 та швидкість каналу 128’000.

Router_IPS(config)#interface s0/1/0

Router_IPS(config-if)#bandwidth 128

Router_IPS(config-if)# clock rate 128000

3.4 Налаштування та перевірка роботи комп'ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Процес базового налаштування конфігурації активних мережних пристроїв включає:

- застосування сервісу шифрування паролів;
- захист привілейованого режиму ОС, консольного порту та ліній vty;
- призначення банера MOTD;
- для віддаленого доступу до пристрою на лініях vty застосований протокол SSH;
- створено локальні облікові записи (*username 12319_Anikeev*) з паролем *admincisco12319*;
- створено доменне ім'я пристрою (*ip domain-name R1_Anikeev*);
- створено ключ RSA завдовжки 1024 біт для шифрування даних.

Приклад базових налаштувань на роутері R1.

Заборонено пошук DNS на маршрутизаторі:

Router(config)#no ip domain-lookup

Задання пристрою унікального імені:

Router(config)#hostname R1_Anikeev

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

R1_Anikeev(config)#service password-encryption

Встановлення паролю на вхід до привілейованого режиму:

R1_Anikeev(config)#enable secret class12319

Встановлено парою на вхід до консольної лінії:

R1_Anikeev(config)#line console 0

R1_Anikeev(config-line)#password cisco12319

Налаштування запиту пароля при вході:

R1_Anikeev(config-line)#login

R1_Anikeev(config-line)#exit

Налаштування банера MOTD:

R1_Anikeev(config)#banner motd # 12319 Anikeev. Enter only have key#

Налаштування протоколу SSH, Створення користувача:

R1_Anikeev(config)#username 12319_Anikeev password admincisco;

Створення домену:

R1_Anikeev(config)#ip domain-name R1_Anikeev

Для шифрування даних створено ключ RSA довжиною 1024 біт:

R1_Anikeev(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

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

Налаштування лінії VTY:

R1_Anikeev(config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

R1_Anikeev(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

R1_Anikeev(config-line)#transport input ssh

Встановлення IPv4-адрес відповідно до таблиці 3.3:

R1_Anikeev(config)#interface g0/1

R1_Anikeev (config-if)# ip address 10.22.208.1 255.255.255.0

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

R1_Anikeev(config-if)#no shutdown

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Згідно технічних вимог, в мережі кіберфізичної системи виготовлення вершкового масла для Вінницького молочного заводу «Рошен»

використовується протокол динамічної маршрутизації OSPF 23. 23 – номер автономної системи, це сукупність мереж під єдиним адміністративним управлінням, що забезпечує загальну для всіх вхідних в автономну систему маршрутизаторів політику маршрутизації.

OSPF має такі переваги:

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

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

Включити протокол OSPF на маршрутизаторі командою:

Router_IPS(config)#router ospf 23

Задати ідентифікатор маршрутизатора (router ID) – унікальне 32-бітове число, яке унікально ідентифікує маршрутизатор в межах однієї автономної системи.

Router_IPS(config)#router-id 17.17.17.17

Протоколу потрібно об’явити мережі, підключені до маршрутизатора.

Router_IPS(config-router)#network 10.68.0.0 0.0.0.127 area 0

Router_IPS(config-router)#network 10.0.10.8 0.0.0.3 area 0

*area 0 – з*она (area) – сукупність мереж і маршрутизаторів, що мають один і той же ідентифікатор зони.

Виконаємо перевірку таблиць маршрутизацій на маршрутизаторах. Кожний маршрутизатор окрім безпосередньо підключених мереж з символом «С» має відомості про всі віддалені мережі, отримана по протоколу OSPF з

символом «O». Також мають записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS.

```
Gudakov_R4#sh ip ro
Gudakov_R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.10.0/30 [110/15064] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.0.10.4/30 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.9/32 is directly connected, Serial0/0/1
C       10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L       10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C       10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L       10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C       10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L       10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C       10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L       10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O       10.68.0.128/25 [110/15065] via 10.0.10.10, 00:03:06, Serial0/0/1
O       10.68.1.0/26 [110/65] via 10.0.10.10, 00:03:16, Serial0/0/1
O       10.68.1.64/27 [110/7565] via 10.0.10.10, 00:03:06, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7564] via 10.0.10.10, 00:03:16, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.3– Таблиця маршрутизації на Router_IPS

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

3.4.3 Налаштування роботи Інтернет

access-list 5 permit 10.0.0.0 0.255.255.25

ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

ip nat inside source list 5 pool Internet overload

ip nat inside source static ***10.23.0.200*** *209.165.200.5*

interface s0/1/0

ip nat inside

inter s0/1/1

ip nat in

int s0/3/0

ip nat inside

inter s0/3/1

ip nat outside

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 10.22.210.10 255.255.255.0 – адреса Server HTTP;
- номер списку доступу: 5;
- ім'я пулу: Internet.

Приклад налаштування NAT на Anikeev_R3:

Список контролю доступу, що дозволяє всі адреси внутрішньої мережі:

Anikeev_R3(config)# access-list 5 permit 10.68.0.0 0.0.3.255

Пул для динамічного виділення інтернет адрес:

Anikeev_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224

Підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу:

Anikeev_R3(config)#ip nat inside source list 6 pool Internet

Адреса статичного NAT для серверу HTTP:

Anikeev_R3(config)#i ip nat inside source static 10.68.0.149 209.165.200.5

Призначення інтерфейсу в якості вихідного для трафіку з мережі приватних адрес:

Anikeev_R3(config)#interface F4/0

Anikeev_R3(config-if)#ip nat outside

Призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес:

Anikeev_R3(config-if)#interface Serial2/0

Anikeev_R3(config-if)#ip nat inside

Для перевірки роботи NAT отримаємо таблицю перетворювань.

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.12:1	10.68.0.140:1	209.165.202.1:1	209.165.202.1:1
icmp	209.165.202.11:1	10.68.0.141:1	209.165.202.1:1	209.165.202.1:1
icmp	209.165.202.8:1	10.68.1.15:1	209.165.200.5:1	209.165.200.5:1
icmp	209.165.202.8:2	10.68.1.15:2	209.165.200.5:2	209.165.200.5:2
icmp	209.165.202.9:1	10.68.1.79:1	209.165.200.5:1	209.165.200.5:1
icmp	209.165.202.10:1	10.68.1.82:1	209.165.202.1:1	209.165.202.1:1
---	209.165.200.5	10.68.0.149	---	---

Рисунок 3.4 – Таблиця перетворювань NAT на Anikeev_R3

3.4.4 Перевірка роботи комп’ютерної системи

Пінгування хостів між підмережами LAN2 та LAN1.

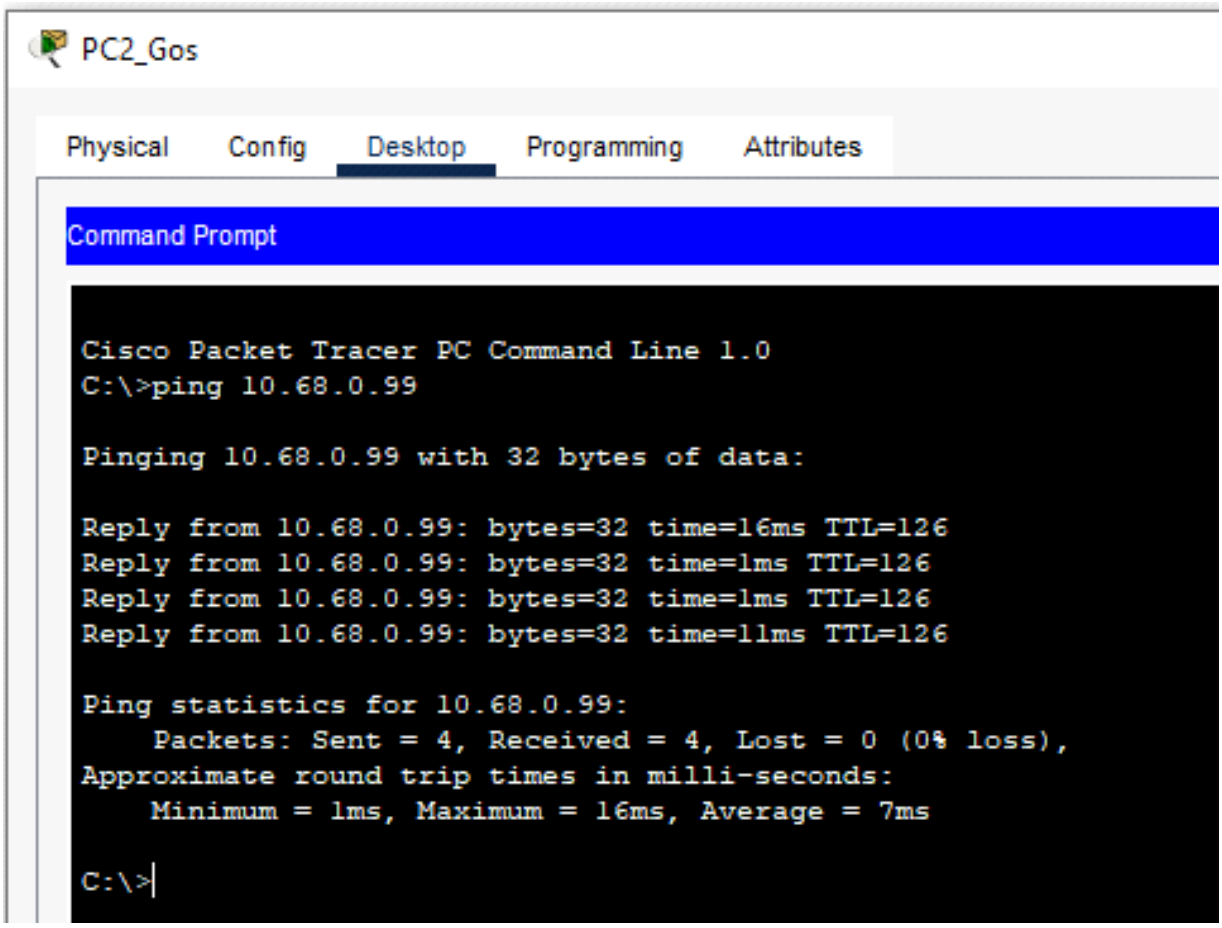


Рисунок 3.5 – Результат команди «ping» між підмережами КС

Для перевірки SSH зробимо підключення з командного рядка Gl_Engineer з підмережі «LAN4» до маршрутизатора R1_Anikeev від користувача 12319_Anikeev з паролем admincisco12319 командою *ssh –l username ip-address*.

В підмережах хости отримують мережні налаштування за протоколом DHCP.

Приклад налаштування DHCP на R2_Anikeev.

R2_Anikeev(config)#interface g0/1

Активовано протокол DHCP:

R2_Anikeev(config-if)#service DHCP

Створений пул DHCP з ім’ям Organization_department:

R2_Anikeev(config-if)#ip dhc pool LAN1

Вилучено з пулу перші 10 адрес:

R2_Anikeev(config-if)#ip dhc ex 10. 68.0.32 10. 68.0.42

Зазначена мережа і шлюз за замовчуванням:

R2_Anikeev(config-if)#net 10.68.0.32 255.255.255.224

R2_Anikeev(config-if)#def 10.68.0.33

R2_Anikeev(config-if)#dns 10.68.10.10

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.68.0.34	0002.1722.B3AD	--	Automatic
10.68.0.35	0007.EC39.1261	--	Automatic
10.68.0.36	0001.9720.2C99	--	Automatic
10.68.0.66	00E0.B016.BC25	--	Automatic
10.68.0.67	0000.0C78.964D	--	Automatic
10.68.0.68	0060.5C72.13EA	--	Automatic
10.68.0.99	000C.CF94.17A9	--	Automatic
10.68.0.98	00D0.BAA1.008D	--	Automatic
10.68.0.100	0060.7041.7427	--	Automatic

Рисунок 3.5 – Таблиця призначення IP-адрес вузлам за протоколом DHCP

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Дослідимо механіку захисту комп'ютерної інформації від несанкціонованого використання або модифікації.

Захист концентрується на апаратних або програмні пристроях – які необхідні для підтримки захисту інформації.

Для цього треба розглянути три основні пункти:

- бажані функції, принципи проектування та приклади елементарних механізмів захисту та аутентифікації;
- архітектуру комп'ютера на основі дескрипторів з використанням сучасної архітектури захисту та зв'язку між системами можливостей та системами контролю доступу, аналізом охоронюваних підсистем та об'єктів, що охороняються;
- сучасний стан та поточні дослідницькі проекти.

Наведемо глосарій для довідки про короткі визначення для декількох термінів, які широко використовуються в контексті захисту інформації в комп'ютерах.

Access – можливість використовувати інформацію, що зберігається в комп'ютерній системі. Часто використовується як дієслово, до жаху граматиків.

Access control list – список довірителів, яким дозволено мати доступ до певного об'єкта.

Authenticate – перевірка особи (або іншого агенту, зовнішнього по відношенню до системи захисту), яка робить запит.

Authorize – надання довірителю доступу до певної інформації.

Capability – незаперечний доказ того, що ведучий уповноважений має доступ до об'єкта, зазначеного в квитку.

Certify – для перевірки точності, правильності та повноти механізму безпеки або захисту.

Complete isolation – система захисту, яка розділяє принципали на відсіки, між якими неможливий потік інформації або управління.

Confinement – надання позиковій програмі доступу до даних, гарантуючи, що програма не зможе оприлюднити інформацію.

Descriptor – захищена величина, яка є (або призводить до) фізичної адреси деякого об'єкта, що охороняється.

Discretionary – (на відміну від недискреційних) – контроль доступу до об'єкта, який може бути змінений творцем об'єкта.

Domain – набір об'єктів, до яких наразі може отримати прямий доступ довіритель.

Encipherment – (зазвичай) оборотне скремблювання даних відповідно до секретного ключа перетворення, щоб зробити їх безпечними для передачі або зберігання у фізично незахищеному середовищі.

Grant – для авторизації.

Hierarchical control – посилаючись на можливість змінювати авторизацію, схему, в якій запис кожного дозволу контролюється іншим дозволом, що призводить до ієрархічного дерева авторизацій.

List-oriented – використовується для опису системи охорони, в якій кожен об'єкт, що охороняється, має перелік уповноважених довірителів.

Password – рядок секретних символів, який використовується для автентифікації заявленої особи особи.

Permission – особлива форма дозволеного доступу, наприклад, дозвіл ЧИТАТИ на відміну від дозволу WRITE.

Prescript – правило, якого необхідно дотримуватися, перш ніж дозволити доступ до об'єкта, тим самим вводячи можливість для людського судження про необхідність доступу, щоб не допускати зловживання доступом.

Principal – суб'єкт господарювання в комп'ютерній системі, якому надаються дозволи; таким чином, одиниця підзвітності в комп'ютерній системі.

Privacy – здатність фізичної особи (або організації) вирішувати, чи, коли і кому передається особиста (або організаційна) інформація.

Propagation – коли довіритель, отримавши санкціонований доступ до якогось об'єкта, в свою чергу дозволяє доступ до іншого довірителя.

Protected object – структура даних, існування якої відомо, але внутрішня організація якої недоступна, окрім як шляхом виклику захищеної підсистеми, яка керує нею.

Protected subsystem – сукупність процедур та об'єктів даних, інкапсульована у власній області таким чином, що внутрішня структура об'єкта даних доступна лише процедурам захищеної підсистеми, а процедури можуть викликатися лише у визначених точках входу домену.

Protection – безпека, використовується більш вузько для позначення механізмів і прийомів, що контролюють доступ виконуваних програм до збереженої інформації.

Protection group – принципал, яким можуть користуватися кілька різних осіб.

Revoke – відібрати раніше санкціонований доступ у якогось принципала.

Security – що стосується систем обробки інформації, використовується для позначення механізмів і методів, які контролюють, хто може використовувати або модифікувати комп'ютер або інформацію, що зберігається в ньому.

Self control – посилаючись на можливість змінювати авторизацію, схему, в якій кожен дозвіл містить у собі специфікацію того, які принципи можуть його змінювати.

Ticket-oriented – використовується для опису системи захисту, в якій кожен принципал веде список незабутніх бітових шаблонів, званих квитками, по одному для кожного об'єкта, до якого принципал має право доступу.

User – використовується неточно для позначення особи, яка несе відповідальність за деякий ідентифікований набір дій у комп'ютерній системі.

3.5.1.1 Основні принципи захисту інформації

1) Загальні примітки: Коли комп'ютери стають краще зрозумілими та економічними, щодня з'являються нові програми. Багато з цих нових додатків передбачають як зберігання інформації, так і одночасне використання багатьма людьми. Основною проблемою цього документа є повторне використання. Для тих програм, в яких не всім користувачам потрібні однакові повноваження, потрібна певна схема для забезпечення того, щоб комп'ютерна система реалізувала необхідну структуру харчування.

Щодня зустрічається безліч інших прикладів систем, які вимагають захисту інформації: банки даних кредитних бюро. Інформаційні системи для правоохоронних органів; офіс-шерінг; медичні інформаційні онлайн-системи; система обробки даних для державних соціальних служб. Ці приклади

охоплюють широкий спектр організаційних та особистих потреб у конфіденційності. Всі вони мають контрольований спільний обмін інформацією між декількома користувачами. Таким чином, кожному потрібен якийсь план, щоб переконатися, що комп'ютерна система допомагає в реалізації правильної структури харчування. Звичайно, деякі програми не вимагають особливих положень в комп'ютерній системі. Наприклад, може статися так, що збережена інформація належним чином захищена через зовнішнього етичного кодексу або відсутності знань про комп'ютери. Хоча бувають випадки, коли комп'ютеру не потрібні будь-які допоміжні засоби для забезпечення захисту інформації.

Слова «конфіденційність», «безпека» і «безпека» часто використовуються по відношенню до систем зберігання інформації. Не всі автори використовують ці терміни однаково. У цій статті використовуються загальні визначення в літературі з інформатики.

Термін «конфіденційність» відноситься до соціально обумовленої здатності особи (або організації) вирішувати, коли і для кого ділитися особистою (або організаційною) інформацією.

Термін «безпека» описує способи, за допомогою яких ви контролюєте, хто може використовувати або змінювати ваш комп'ютер, або інформацію на ньому.

1) Несанкціоноване розповсюдження інформації: Будь-яка неуповноважена особа може читати та використовувати інформацію, що зберігається на комп'ютері. Ця категорія тривоги іноді поширюється на «аналіз трафіку», в якому зловмисник спостерігає лише закономірності використання інформації та може зробити висновок про певний інформаційний зміст із цих моделей. Це також включає несанкціоноване використання невільної програми.

2) Несанкціонована зміна інформації: Будь-яка стороння особа може внести зміни до збереженої інформації – форма саботажу. Зверніть увагу, що це порушення не вимагає від зловмисника бачити інформацію, яку він змінив.

3) Відмова від несанкціонованого використання: Зловмисник може перешкодити авторизованому користувачеві отримати доступ або змінити інформацію, навіть якщо зловмисник не може отримати доступ або змінити інформацію. Прикладами відмови від використання є системний «збій», порушення алгоритму планування або стрілянина по комп'ютеру. Це ще одна форма навернення.

Термін «несанкціонований» в перерахованих вище трьох категоріях означає, що розкриття, зміна або відмова від використання відбувається проти волі особи, яка контролює інформацію, і може вступати в протиріччя з обмеженнями, нібито накладеними системою. Найбільша складність комп'ютерної системи загального призначення з віддаленим доступом полягає в тому, що «зловмисником» в цих визначеннях може бути законний користувач комп'ютерної системи.

Нижче наведені приклади технологій безпеки, які іноді застосовуються до комп'ютерних систем: позначення файлів списками авторизованих користувачів, перевірка особистості потенційного користувача запитом пароля, захист комп'ютера для запобігання перехоплення електромагнітного випромінювання і подальшої інтерпретації, шифрування інформації, що передається по телефонних лініях, блокування приміщення, де знаходиться комп'ютер, контроль того, кому дозволено вносити зміни в комп'ютерну систему (наприклад, її апаратне і програмне забезпечення), а також використання резервних ланцюжків Або запрограмовані перевірки, які підтримують безпеку в умовах апаратних або програмних збоїв, засвідчуючи, що апаратне та програмне забезпечення вже виконуються за призначенням.

Очевидно, що широке коло міркувань стосується інженерної безпеки інформації. Історично склалося так, що в літературі про комп'ютерні системи термін «безпека» вузько визначався тільки як методи безпеки, які контролюють доступ виконуваних програм до збереженої інформації.3 Прикладом методу

захисту є маркування файлів, що зберігаються на комп'ютері, списками авторизованих користувачів. . Аналогічно, термін аутентифікація використовується для тих методів безпеки, які перевіряють особистість особи (або іншого зовнішнього агенту), який робить запит до комп'ютерної системи. Прикладом методики аутентифікації є запит пароля. У цій статті мова піде про механізми безпеки і аутентифікації, і згадуються лише інші, не менш важливі механізми безпеки.

Слід визнати, що зосередження уваги на механізмах безпеки та документації забезпечує вузьке уявлення про інформаційну безпеку, і що вузьке бачення є небезпечним. Метою захищеної системи є запобігання будь-якому несанкціонованому використанню інформації, яка є негативною вимогою. Довести, що ця негативна умова була дотримана, складно, так як необхідно довести, що всі можливі загрози були передбачені. Таким чином, широкий погляд на проблему найкраще підходить для того, щоб в стратегії не було прогалин. Навпаки, вузька спрямованість на захисні механізми, особливо ті, які логічно неможливо подолати, може призвести до хибної довіри до системи в цілому.

2) Функціональні рівні інформаційної безпеки: запропоновано багато різних конструкцій і реалізовано механізми захисту інформації в комп'ютерних системах. Однією з причин відмінностей схем захисту є їх різні функціональні характеристики – види контролю доступу, які можуть виражатися як природно, так і примусово. Схеми захисту зручно розділити за функціональними характеристиками. Приблизна класифікація виглядає наступним чином.

а) Незахищені системи: Деякі системи не мають засобів, щоб запобігти доступу конкретного користувача до всієї інформації, що зберігається в системі. Тут важливе наше визначення захисту, яке виключає функції, які можна використовувати лише для запобігання помилкам, оскільки небезпечні системи зазвичай мають різноманітні функції запобігання помилкам. Він може

забезпечити достатній контроль, щоб будь-яке порушення контролю могло бути результатом навмисної дії, а не нещасним випадком. Однак було б неправильно стверджувати, що такі системи забезпечують будь-який вид безпеки

b) системи «Все або нічого»: ці системи забезпечують ізоляцію користувача, а іноді контролюються шляхом повного обміну певною інформацією. Тільки при забезпеченні ізоляції користувач такої системи може використовувати власний комп'ютер для захисту та обміну інформацією. Найчастіше в цих системах також є публічні бібліотеки, до яких може звернутися кожен користувач. У деяких випадках механізм публічної бібліотеки може бути розширений для прийняття внесків користувачів, але все одно на основі того, що всі користувачі мають рівний доступ. Більшість комерційних систем розподілу часу першого покоління забезпечують схему захисту з таким рівнем функціональності.

c) Контрольований обмін: необхідна більш складна технологія, щоб чітко контролювати, хто може отримати доступ до кожного елемента даних, що зберігається в системі. Наприклад, така система може надати кожному файлу список авторизованих користувачів і дозволити власнику виділити кілька типових шаблонів використання, таких як читання вмісту файлу, їх запис або виконання у вигляді програми.

e) Запрограмовані користувачем елементи керування спільним доступом: користувач може захотіти обмежити доступ до файлу таким чином, як це не передбачено стандартними елементами керування спільним доступом. Наприклад, доступ може бути дозволений тільки в будні дні з 9:00 ранку. А 16:00 може захотіти дозволити доступ лише до середнього значення даних у файлі. Може бути, він хоче попросити відредагувати файл тільки за згодою двох користувачів.

Для таких і багатьох інших випадків загальним рішенням є надання захищених об'єктів і підсистем, визначених користувачем. Захищена підсистема

– це сукупність програм і даних з властивістю, що безпосередній доступ до даних (тобто об'єктів, що охороняються) мають лише програми-підсистеми. Доступ до цих програм обмежений підключенням до зазначених точок входу. Таким чином, програми підсистеми повністю контролюють операції, що виконуються над даними. Після побудови захищеної підсистеми користувач може розробити будь-яку програмовану форму для управління доступом до створених ним об'єктів. Лише кілька більш просунутих конструкцій систем намагалися дозволити визначені користувачем захищені підсистеми.

Вивчення альтернативних механізмів реалізації захищених підсистем є актуальною темою досліджень. Спеціалізованим використанням захищених підсистем є здійснення контролю безпеки на основі змісту даних. Наприклад, у файлі заробітної плати ви можете надати доступ до всіх зарплат до 15 000 доларів. Іншим прикладом є надання доступу до певних статистичних наборів даних, але не до будь-якого окремого елемента даних. Ця сфера захисту ставить питання про можливість розрізнення інформації за допомогою статистичних тестів і вивчення показників без прямого доступу до самих даних. Захист на основі вмісту є предметом низки нещодавніх або поточних дослідницьких проектів і не розглядатиметься в цьому посібнику.

д) Додавання рядків до інформації: Вищезазначені три рівні свідчать про встановлення умов для передачі інформації реалізованій програмі. Четвертий рівень здатності полягає в тому, щоб зберігати певний контроль над користувачем інформації навіть після її оприлюднення. Такий контроль бажаний, наприклад, при наданні інформації про доходи податковому консультанту; обмеження повинні перешкоджати його передачі інформації компанії, що готує списки розсилки. Ще одним прикладом обмеження доступу до інформації після її передачі особі, уповноваженій на її отримання, є написи, надруковані на секретній військовій інформації з оголошенням документа «цілком таємно».

Заборонено (без ризику суворого покарання) передавати цю інформацію оточуючим, а ярлик служить повідомленням про обмеження. Комп'ютерні системи, що реалізують такі лінії інформації, дефіцитні, а механізми неповні. Наприклад, система відстежує рівень класифікації всіх вхідних даних, що використовуються для створення файлу; всі необроблені дані автоматично позначаються найвищим рейтингом, що зустрічається під час виконання.

Існує міркування, яке стосується всіх рівнів функціональності: динаміка використання. Цей термін стосується того, як ви визначаєте, хто може отримувати доступ до створених елементів і змінювати їх. На будь-якому рівні відносно легко уявити (і спроектувати) системи, які послідовно виражають той чи інший захисний намір. Але необхідність динамічної зміни ліцензії доступу і необхідність запиту таких змін за допомогою впровадження програм істотно ускладнюють системи безпеки. Для цього функціонального рівня більшість існуючих систем захисту принципово відрізняються тим, як вони справляються з динамікою захисту. Повинно бути зрозуміло, що положення про динаміку використання не менш важливі, ніж положення про фіксовані специфікації захисного наміру.

У багатьох випадках немає необхідності задовольняти потреби в захисті особи, відповідальної за інформацію, що зберігається в комп'ютері за допомогою комп'ютерного управління. Зовнішні механізми, такі як контракти, незнання або паркани з колючого дроту, можуть забезпечити деякі необхідні функції. Однак ця дискусія зосереджена на внутрішніх механізмах.

g) Принципи проектування: Незалежно від рівня функціональності, що надається, корисність набору механізмів захисту залежить від здатності системи запобігати порушенням безпеки. На практиці доведено, що створити систему для будь-якого рівня функціональності (крім першого) дійсно запобігає подібні несанкціоновані дії досить складно. Досвідчені користувачі більшості систем знають як мінімум один спосіб порушити роботу системи, відмовивши іншим

користувачам в санкціонованому доступі до збереженої інформації. Навчання проникненню за участю великої кількості різних систем загального призначення показало, що користувачі можуть створювати програмне забезпечення, яке має несанкціонований доступ до інформації, що зберігається в них. Навіть у системах, розроблених та впроваджених з урахуванням безпеки як важливої мети, дефекти проектування та впровадження забезпечують способи обійти передбачувані обмеження доступу.

Методи проектування і будівництва, систематично усувають недоліки, є предметом багатьох наукових робіт, але жоден повний метод не застосовується до побудови великих систем загального призначення. Ця складність пов'язана з негативною якістю вимог щодо запобігання будь-яких несанкціонованих дій

За відсутності цих методологічних прийомів досвід надав деякі корисні принципи, які можуть керувати розробкою та сприяти впровадженню без недоліків безпеки. Ось вісім прикладів принципів проектування, які особливо актуальні для захисних механізмів.

a) Механізм економії: Зберігайте конструкцію максимально простою та компактною. Цей відомий принцип можна застосувати до будь-якого аспекту системи, але звернути увагу на механізми захисту варто саме з цієї причини: помилки проектування і реалізації, які призводять до небажаних шляхів доступу, при звичайному використанні спостерігатися не будуть (так як нормальне використання зазвичай не передбачає спроб використання неправильних шляхів доступу). В результаті потрібні такі методи, як перевірка програми часу і фізична перевірка пристроїв, що реалізують механізми безпеки. Для того щоб ці способи спрацювали, необхідна невелика і проста конструкція.

b) Відмовостійкі дефолти: на основі точності, а не винятків. Консервативний дизайн повинен ґрунтуватися на аргументах, які роблять речі доступними, а не на тому, чому до них не слід звертатися. У великій системі деякі активи будуть розглядатися неадекватно, тому безпечно не мати дозволу

за замовчуванням. Помилка проектування або впровадження в механізмі, який надає явний дозвіл, як правило, зазнає невдачі через відмову в дозволі, безпечну ситуацію, коли вона буде швидко виявлена. З іншого боку, помилка проектування або реалізації в механізмі, який явно виключає доступ, зазвичай призводить до збою, дозволяючи доступ, збій, який може залишитися непоміченим при звичайному використанні. Цей принцип стосується як зовнішнього вигляду захисного механізму, так і його основної реалізації.

c) Повне посередництво: кожна заявка на кожен об'єкт повинна бути перевірена на обґрунтованість. Цей принцип, якщо застосовувати його систематично, є базовою основою системи захисту. Він забезпечує загальносистемний огляд контролю доступу, який крім нормальної роботи включає ініціалізацію, відновлення, відключення і технічне обслуговування. Це означає, що необхідно розробити надійний метод визначення джерела кожного замовлення. Це також вимагає, щоб пропозиції щодо підвищення продуктивності шляхом збереження результатів сертифікаційного тесту розглядалися зі скептицизмом. Якщо відбувається зміна влади, ці пам'ятні результати слід систематично оновлювати.

d) Відкритий дизайн: дизайн не повинен бути конфіденційним. Механізми повинні покладатися не на незнання потенційних зловмисників, а на більш легке володіння специфічними і безпечними ключами або паролями. Таке розділення механізмів безпеки та перемикачів безпеки дозволяє багатьом аудиторам досліджувати механізми, не побоюючись, що сама перевірка може поставити під загрозу гарантії. Крім того, будь-якому скептично налаштованому користувачеві можна дозволити переконати себе в тому, що система, яку він має намір використовувати, підходить для їх цілей.9 Нарешті, просто нереально намагатися зберегти в таємниці будь-яку систему, яка набула широкого поширення.

e) Поділ привілеїв: Якщо можливо, механізм безпеки, який вимагає двох ключів розблокування, є більш надійним і гнучким, ніж механізм, який дозволяє отримати доступ до заявника лише одним ключем. Система оборони також має ядерну зброю, стріляючи тільки тоді, коли дві різні людини дають правильну команду. У комп'ютерній системі окремі ключі застосовуються до будь-якої ситуації, коли необхідно виконати дві або більше умов, перш ніж можна буде дозволити доступ. Наприклад, системи, які надають розширювані користувачем типи даних, зазвичай покладаються на спільний доступ до привілеїв для їх реалізації.

f) Найменший набір привілеїв: кожна програма і кожен користувач системи повинні працювати з використанням найменшого набору привілеїв, необхідних для виконання завдання. Перш за все, цей принцип обмежує збитки, які можуть виникнути в результаті аварії або несправності. Це також зменшує кількість потенційних взаємодій між преміальними додатками до мінімуму для належної роботи, тому ймовірність ненавмисного, небажаного або неналежного використання привілеїв нижча. Таким чином, якщо виникає питання про зловживання привілеями, кількість програм, що підлягають аудиту, скорочується. Іншими словами, якщо механізм може надавати «брандмауери», принцип менших привілеїв забезпечує обґрунтування того, де встановлені брандмауери. Прикладом цього принципу є правило військової безпеки «обов'язково знати».

g) Менш загальний механізм: зменшення кількості механізмів, спільних для багатьох користувачів, від яких залежать усі користувачі. Кожен загальний механізм (особливо той, що включає загальні змінні) являє собою потенційний шлях інформації між користувачами і повинен бути розроблений з великою обережністю, щоб гарантувати, що він випадково не порушить безпеку. Крім того, будь-який механізм, який обслуговує всіх користувачів, повинен бути прийнятий для задоволення кожного користувача, що, мабуть, складніше, ніж

задовольнити лише одного користувача або кількох користувачів. Наприклад, якщо ви вирішили застосувати нову функцію як контрольовану дію, спільну для всіх користувачів, або як дію бібліотеки, якою можна керувати так, ніби нею можна керувати, виберіть останній курс. Потім, якщо один або кілька користувачів не задоволені рівнем автентифікації функції, вони можуть замінити її або взагалі не використовувати. У будь-якому випадку вони зможуть уникнути пошкодження через помилку в ньому.

h) Психологічне прийняття: Важливо, щоб людський інтерфейс був розроблений для простоти використання, щоб користувачі регулярно та автоматично правильно застосовували механізми захисту. Крім того, в тій мірі, в якій уявлення користувача про його цілях захисту відповідають механізмам, які він повинен використовувати, помилки будуть зведені до мінімуму. Якби йому довелося перекласти своє уявлення про свої потреби в захисті на мову, радикально відмінну від специфікації, він би зробив помилки.

Аналітики традиційних систем фізичного захисту запропонували ще два принципи проектування, які, на жаль, не в повній мірі застосовуються до комп'ютерних систем.

a) Фактор роботи: Порівняйте вартість обходу механізму з ресурсами потенційного зловмисника. Вартість трудівника, в деяких випадках можна легко розрахувати. Наприклад, кількість експериментів, необхідних для випробування всіх можливих чотиризначних паролів, становить 2^{64}. Якщо потенційному зловмиснику доводиться вводити кожен пробний пароль на пристрої, можна припустити, що досить чотиризначного пароля. З іншого боку, якщо зловмисник може використовувати великий комп'ютер, здатний спробувати мільйон паролів в секунду, як у випадку з промисловим шпигунством або військовою безпекою, пароль з чотирьох букв стане незначною перешкодою для потенційного зловмисника.

Проблема принципу дії трудового фактору полягає в тому, що багато механізмів комп'ютерного захисту не підлягають прямому розрахунку трудящого, так як перемогти їх систематичною атакою може бути логічно неможливо. Поразки можна досягти тільки за допомогою непрямих стратегій, таких як очікування випадкового апаратного збою або пошук помилки виконання. Дуже складно зробити достовірні оцінки тривалості цього очікування або дослідження.

б) Скомпрометований запис: іноді передбачається, що механізми, які надійно фіксують факт витоку інформації, можуть бути використані замість більш складних механізмів, які запобігають втраті взагалі. Наприклад, якщо ви знаєте, що тактичний план зламаний, ви можете створити інший план, який зробить зламану версію марною. Приклад такого механізму - непорушний замок на хисткому картотеці. Хоча інформацію, що зберігається всередині, легко відновити, сховище неминуче буде пошкоджено в процесі, і наступний законний користувач виявить втрату.

Інший приклад: багато комп'ютерних систем записують дату і час останнього використання кожного файлу. Якщо цей журнал стійкий до злому та повідомлений власнику, він може допомогти виявити несанкціоноване використання. У комп'ютерних системах такий підхід використовується рідко, так як важко забезпечити виявлення після порушення безпеки. Фізичні пошкодження зазвичай не задіяні, а логічні пошкодження (і журнали перешкод, що зберігаються всередині) можуть бути обійдені спритним зловмисником.

Як зрозуміло, ці принципи не є абсолютними правилами - вони найкраще служать попередженнями. Якщо будь-яка частина проекту порушує принцип, це порушення є симптомом потенційної проблеми, і проект повинен бути ретельно переглянутий, щоб переконатися, що проблема була вирішена або не актуальна.

Коротше кажучи, ми можемо довести нашу дискусію до цього моменту. Використання комп'ютерів для вирішення завдань обробки інформації вимагає

різноманітних механізмів безпеки. Ми акцентуємо увагу на одному аспекті - механізмах комп'ютерного захисту – механізмах, які контролюють доступ до інформації за допомогою реалізації програм. Можна визначити принаймні чотири рівні функціональності системи безпеки: система «все або нічого», контрольований спільний доступ, запрограмовані користувачем елементи керування спільним доступом та інформаційні рядки. Але на всіх рівнях забезпечення динамічних змін авторизації доступу представляє серйозну складність.

Оскільки ніхто не знає, як побудувати бездоганну систему, альтернативою є опора на вісім принципів проектування, які прагнуть зменшити кількість і серйозність будь-яких дефектів: ефективність механізму, відмовостійкі параметри за замовчуванням, повна медіація, відкритий дизайн, поділ привілеїв, найменші привілеї, менш поширені механізми та психологічна прийнятність.

Нарешті, деякі комбінації безпеки можна оцінити, порівнявши ресурси потенційного зловмисника з фактором дії, необхідним для перемоги над системою, і оцінка компромісу може бути корисною стратегією.

3.5.2 Налаштування маршрутизаторів на підтримку служби AAA

Приклад налаштування сервісу AAA та сереверу RADIUS.

Запуск служби AAA:

Router_IPS(config)#aaa new-model

Налаштування методу аутентифікації з використання локальної бази користувачів:

Router_IPS(config)#aaa authentication login default local

Налаштування методу аутентифікації Login на серевері RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів:

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

Застосування методу аутентифікайфії Login на консольній лінії та vty:

Router_IPS(config)#line console 0

Router_IPS(config-line)#login authentication Login

Router_IPS(config)#line vty 0 4

Router_IPS(config-line)#login authentication default

Налаштування RADIUS-серверу:

Router_IPS(config)#radius-server host 10.68.10.10 auth-port 1645

Router_IPS(config)#radius-server key Radius+Anikeev123

Для доступу використовується доменне ім’я пристрою Anikeev_R3 з паролем Radius+Anikeev123, що був налаштований на сервері RADIUS.

На портах комутатора, де підключені сервери кіберфізичної системи виготовлення вершкового масла для Вінницького молочного заводу «Рошен», налаштовані засоби безпеки: тільки одному вузлу дозволений доступ до порту; MAC-адреса пристрою додається статично в поточну конфігурацію; при порушенні системи безпеки порт виключається.

3.5.3 Налаштування віртуальної приватної мережі VPN

В кіберфізичній системі виготовлення вершкового масла для Вінницького молочного заводу «Рошен» VPN передається трафік між підмережою «LAN2» (шлюзом для неї є інтерфейс роутера Anikeev_R1) та підмережою «LAN3» (шлюзом для неї є інтерфейс роутера Router_IPS).

Для перевірки створеного VPN тунелю передачі трафіку між підмережами застосовується команда *show crypto ipsec sa*.

```
Gudakov_R3#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.10.6

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.68.1.0/255.255.255.192/0/0)
   remote  ident (addr/mask/prot/port): (10.68.1.64/255.255.255.224/0/0)
   current_peer 10.0.10.5 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 8, #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.: 10.0.10.6, remote crypto endpt.:10.0.10.5
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

Рисунок 3.7 – Перевірка стану IPSec SA на роутері Anikeev_R3

4 РОЗРОБКА БАЗА ДАНИХ ЛОГІСТИЧНОГО ЦЕНТРУ "РОШЕН"

4.1 Загальна інформація

Кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» моє розвинуту систему, яка охоплює декілька підрозділів у тому числі і логістичний центр "Рошен".

Автоматизація в сортувальних центрах і складах залишатиметься актуальною темою в найближчі роки, тоді як ручна обробка пакунків і товарів згодом вимре. Все частіше до існуючих будівель додаються гнучкі рішення з можливістю масштабування.

Комп’ютерні системи також стають розумнішими: за допомогою комп’ютерного бачення та Інтернету речей вони не лише повідомляють вам, що відбувається вчора й сьогодні, а й що станеться завтра.

Ключем до еволюції обробки і накопичення інформації є бази даних (БД).

4.2.1 Логістичний центр "Рошен"

Логістичний центр "Рошен" знаходиться в м. Яготині і відповідає всім вимогам до логістичного комплексу класу "А".

Крім готової продукції, в комплексі зберігаються і харчові інгредієнти: кондитерські жири, какао, горіхи, соки і т. д. - всього близько 200 найменувань. Для зберігання кожного з них необхідні свої умови. Працюють холодильники з індивідуальними температурними режимами від +3 до +14 градусів, для соків передбачено морозильники.

Для бездоганного функціонування логістичного комплексу куплено і встановлено складне програмне забезпечення. Функціонує інноваційне транспортне складське устаткування. Для оптимізації транспортування створено ідеально рівну підлогу: погрішність не перевищує 0,3 см на 300 кв. см. Для

оснащення логістичного центру використовується виключно новітнє устаткування передових світових компаній.

Рисунок 4.1 – Логістичний центр "Рошен" (м. Яготин)

Також до складу логістичного центру з 2015 року входить дільниця фасування. Вона сертифікована за ISO 9001 та ISO 22000 [6].

4.2 Розробка бази даних

4.2.1 Постановка завдання для реалізації БД

Для логістичного центру "Рошен" треба розробити БД для систему управління комплексом обладнання власної бензозаправки, яка розташована на території логістичного центру "Рошен".

БД призначена для зберігання основних технологічних параметрів роботи об'єкта.

База даних, що розробляється повинна зберігати таку інформацію:

– інформацію про автоцистерни та водіїв;

– інформацію про прихід палива;

– інформацію про витрати палива;

– загальна кількість палива у сховищі;

– інформацію про операторів і час їх роботи в системі;

– інформація про паливо, що зберігається.

5.2.2 Обґрунтування вибору СУБД

Для реалізації бази даних (БД) для даного дипломного проекту обрана реляційна модель (РМ). В основі РМ лежать прості таблиці, які задовольняють певним обмеженням і можуть розглядатися як математичні відносини. Відносно (таблиці) виділяється декілька атрибутів, однозначно ідентифікують кортежі і званих ключами.

Особливість реляційної моделі полягає в тому, що на відміну від мережевої та ієрархічної моделей реальні об'єкти і взаємозв'язки між ними представляються в базі даних однаково в вигляді нормалізованих відносин.

Переваги реляційної моделі:

- РМ БД є звичним для користувача набором таблиць;
- автоматизований доступ до даних і алгоритми і процедури обробки запитів;
- реляційні мови легкі для вивчення і освоєння;
- реляційне уявлення дає ясну картину взаємозв'язків атрибутів з різних відносин;
- спрямовані зв'язку в реляційної БД відсутні.

- операції проекції і об'єднання дозволяють розрізати і склеювати відносини, що служить для отримання різноманітних файлів в потрібній формі;
- для кожного відносини є можливість завдання правомірності доступу, засекречені показники виділяються в окремі відносини з перевіркою прав доступу.
- фізичне розміщення однорідних файлів набагато простіше, ніж розміщення ієрархічних і мережевих структур.
- БД допускає можливість розширення.

Для управління базою даних в цьому дипломному проекті обрана система керування базами даних Access.

Access сприймає велику кількість форматів даних, включаючи файлові структури інших СУБД. Тому додаток в Access може імпортувати з текстових файлів або електронних таблиць і експорт в них: надавати прямий доступ і оновлювати файли Paradox, FoxPro і інших БД. Можна також імпортувати дані з цих файлів в таблиці Access.

Перевагою Access так само є наявність засобів проектування програми БД без знання мови програмування. Робота в Access починається з визначення реляційних таблиць і полів, призначених для зберігання даних. Відразу після цього за допомогою форм, звітів, макросів і VBA можна визначати дії над цими даними. Форми і звіти використовуються для виведення на екран і додаткових обчислень при роботі з таблицями. У разі розробки більш складного додатка можна використовувати мову Visual Basic.

Вбудована мова запитів SQL дозволяє максимально гнучко працювати з даними і значно прискорює доступ до зовнішніх даних.

Крім того, дана СУБД оптимально підходить під операційну систему, встановлену на АРМ оператора, а саме Microsoft Windows 10.

4.2.3 Розробка логічної структури БД

База даних даного дипломного проекту представлена у вигляді п’яти таблиць: Авто_Інфо – містить інформацію про автоцистерни, які здійснюють перевезення палива до бензозаправки, їх водіїв та ємність цистерн; Прихід_Палива – містить інформацію про паливо, яке надходить на бензозаправку, його кількість та ким привезено; Сховище – містить інформацію про марку палива, яке зберігається на бензозаправці та його кількість; Оператор – містить дані ідентифікації оператора; Витрати_Палива – містить інформацію про паливо, яке реалізовано покупцям, його марку та кількість. Структура таблиць представлена в табл. 4.1.

Таблиця 4.1 – структура таблиць БД

Назва таблиці	Ключ	Поле	Тип	Опис
1	2	3	4	5
Авто_Інфо	так	Авто_Номер	текстовий	номер автомобіля
		Водій_ІПБ	текстовий	ідентифікатор водія
		Цистерна	числовий	ємність цистерни автомобіля, $м^3$
		Наявність_Причіпа	логічний	наявність причіпа
Прихід_Палива	так	Авто_Номер	текстовий	номер автомобіля
		Об’єм_Палива	числовий	інформація про об’єм палива, що надходить
	так	Марка_Палива	текстовий	інформація про марку палива, що надходить
	так	Дата_Приймання	дата/час	дата приймання
	так	Час_Приймання	дата/час	час приймання
Витрати_Палива		Об’єм_Палива	числовий	інформація про об’єм палива, що продається
	так	Марка_Палива	текстовий	інформація про марку палива, що продається
	так	Дата_Відпуску	дата/час	дата приймання
	так	Час_ Відпуску	дата/час	час приймання

Продовження таблиці 4.1

1	2	3	4	5
Сховище	так	Марка_Палива	текстовий	інформація про марку палива, що зберігається
		Об’єм_Сховища	числовий	загальний об’єм

				сховища
Оператор	так	Оператор_ПІБ	текстовый	ідентифікаційні дані оператора
		Дата_Зміни	дата/время	дата входу в систему
		Час_Зміни	дата/время	час входу в систему

Логічна модель бази даних, розроблена в середовищі Access приведена на рис. 4.2.

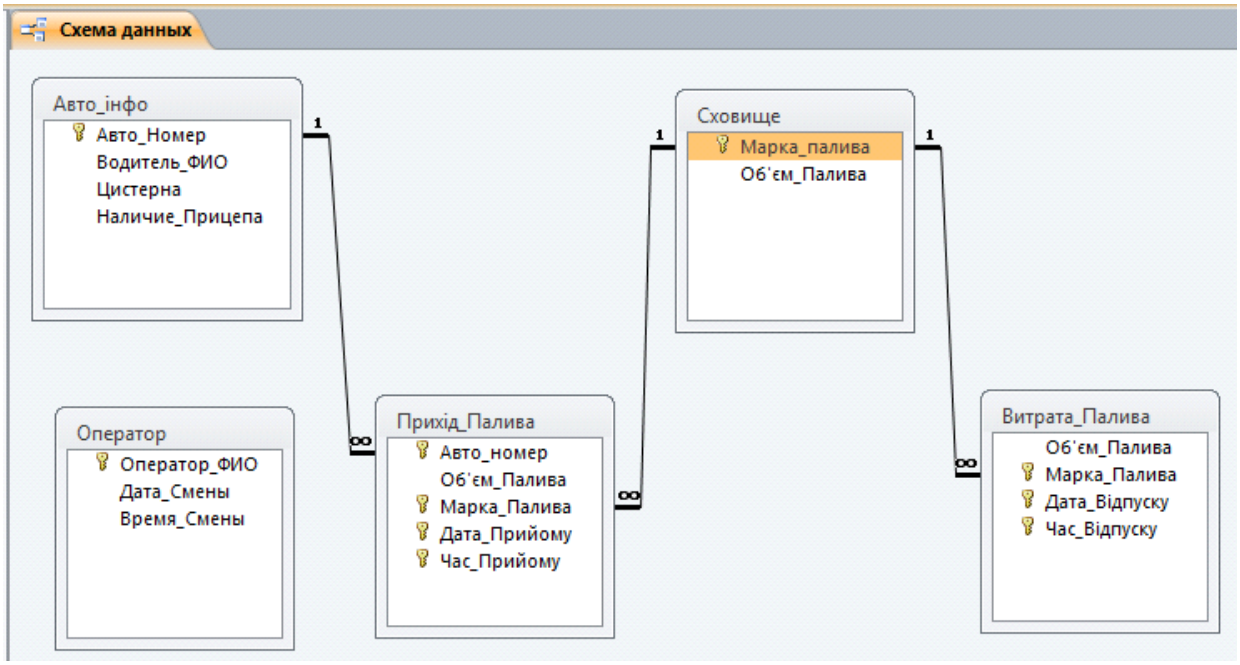


Рисунок 4.2 – Логічна модель бази даних

4.2.4 Створення об'єктів БД

Запит на вибірку інформації про поставку палива та оператора, коли було 15.05.2017 показано на рис. 4.3.

Даному запиту відповідає наступний код на мові SQL:

SELECT DISTINCT Прихід_Палива.*, Авто_інфо.Воддій_ПІБ, Оператор.Оператор_ПІБ

FROM Оператор, (Сховище INNER JOIN Витрата_Палива ON Сховище.Марка_палива = Витрата_Палива.Марка_Палива) INNER JOIN (Авто_інфо INNER JOIN Прихід_Палива ON Авто_інфо.Авто_Номер =

Прихід_Палива.Авто_номер) ON Сховище.Марка_палива = Прихід_Палива.Марка_Палива

WHERE (([Дата_Зміни] Like "15.05.2023"));

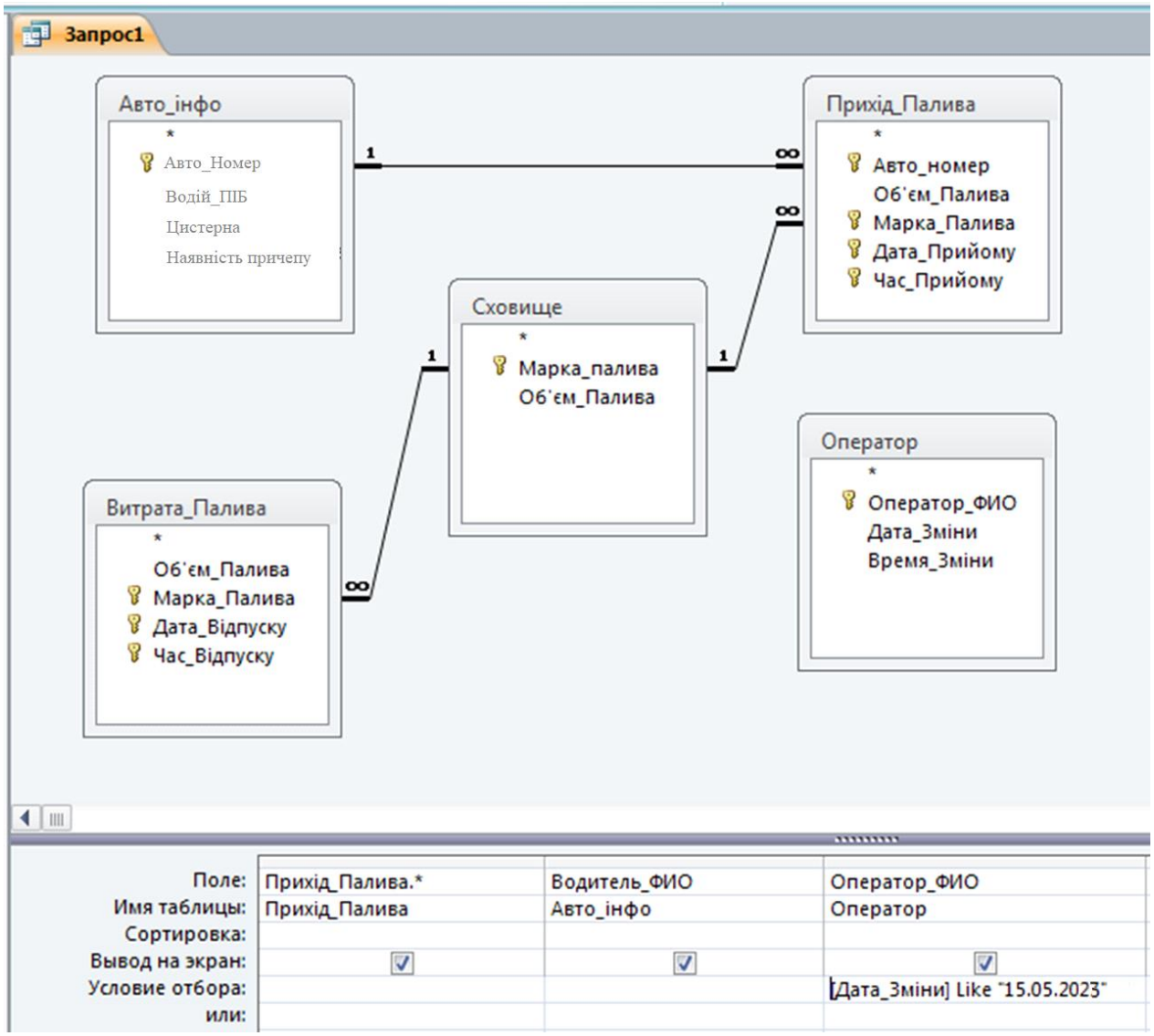
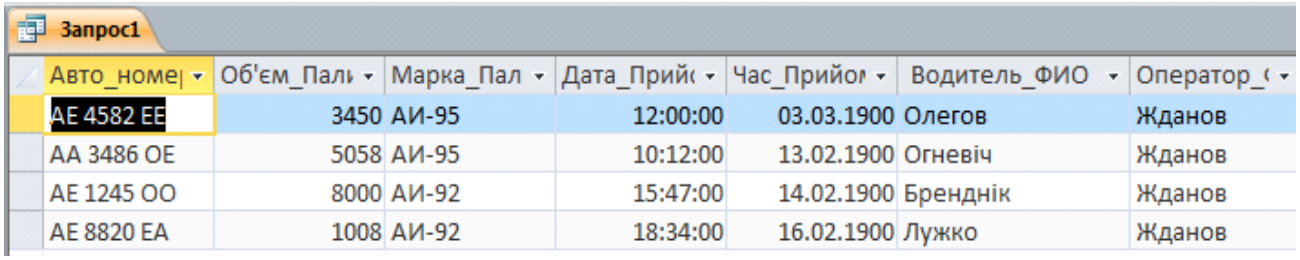


Рисунок 4.3 – Реалізація запиту на вибірку в середовищі Access

Результатом вибірки служить таблиця з інформацією про Запит на вибірку інформації про поставку палива та оператора, коли було 15.05.2023, як зображено на рис. 4.4.



Запрос1

Авто_номе	Об'єм_Пали	Марка_Пал	Дата_Прийо	Час_Прийом	Водитель_ФИО	Оператор_(
АЕ 4582 ЕЕ	3450	АИ-95	12:00:00	03.03.1900	Олегов	Жданов
АА 3486 ОЕ	5058	АИ-95	10:12:00	13.02.1900	Огневіч	Жданов
АЕ 1245 ОО	8000	АИ-92	15:47:00	14.02.1900	Бренднік	Жданов
АЕ 8820 ЕА	1008	АИ-92	18:34:00	16.02.1900	Лужко	Жданов

Рисунок 5.3 – Таблиця результату вибірки

ВИСНОВКИ

Згідно до кваліфікаційної роботи бакалавра необхідно розробити комп’ютерну систему, яка необхідна для впровадження на ПРАТ "Вінницький молочний завод "Рошен" для управління якістю та безпеки харчових продуктів відповідно до вимог міжнародних стандартів ISO 9001 та ISO 22000. Тобто треба розробити кіберфізична систему контролю за підрозділом з виготовленням вершкового масла з детальним опрацюванням побудови і відповідним налаштування корпоративної мережі.

Враховуючи архітектуру кіберфізичної системи з виготовлення вершкового масла для ПРАТ "Вінницький молочний завод "Рошен", попередньою кількість необхідних підмереж, їх взаємозв’язків та кількості комп’ютерів, необхідно розрахувати налаштування для топології мережі,вибрати інтерфейс каналів зв'язку та протоколу обміну,розрахувати топологчну схему комп'ютерної системи,виконати розрахунок комп'ютерної мережі та налаштувань маршрутизації,а також перевірку роботи комп'ютерної системи та подальше моделювання.

У якості об’єкта управління виступає технологічне обладнання маслоутворювачем Тетра Отич ТВФ-2.06 .

В розділі розроблена функціональна схема автоматизації,вибрані апаратно-програмні засоби для створення підсистеми,складений перелік елементів до схеми електричної принципової та розроблена схема принципова підсистеми управління.

У кваліфікаційній роботі бакалавра розроблена кіберфізична система виготовлення вершкового масла для Вінницького молочного заводу «Рошен» з детальним опрацюванням побудови, налаштування корпоративної мережі.

Схема мережі ,яка розроблена та реалізована у вигляді моделі в симуляторі Cisco Packet Tracer перевірена та працює.

Перевірка та її результати у вигляді графіків та таблиць наводяться і описані у пояснювальній записці та додатках.

ПЕРЕЛІК ПОСИЛАНЬ

- Dairy and Food Engineering 3(2+1). Режим доступу: http://ecoursesonline.iasri.res.in/mod/page/view.php?id=1696
- Butter. Режим доступу: https://en.wikipedia.org/wiki/Butter
- Chapter 12. Butter and dairy spreads. Режим доступу: https://dairyprocessinghandbook.tetrapak.com/chapter/butter-and-dairy-spreads
- "Рошен" вінницький молочний завод. Режим доступу: https://vdp-roshen.com.ua/ua/contacts/
- Become a Digital Enterprise and accelerate your digital transformation. Режим доступу: https://www.siemens.com/global/en/products/automation/topic-areas/digital-enterprise.html?acz=1 HYPERLINK "https://www.siemens.com/global/en/products/automation/topic-areas/digital-enterprise.html?acz=1&gclid=Cj0KCQjwyLGjBhDKARIsAFRNgW_1B1Uv2rMiU0JJ77kX_tuL6kweVxyXImvvrPcTGHUTCXy2aaEfnwIaArV3EALw_wcB"& HYPERLINK "https://www.siemens.com/global/en/products/automation/topic-areas/digital-enterprise.html?acz=1&gclid=Cj0KCQjwyLGjBhDKARIsAFRNgW_1B1Uv2rMiU0JJ77kX_tuL6kweVxyXImvvrPcTGHUTCXy2aaEfnwIaArV3EALw_wcB"gclid=Cj0KCQjwyLGjBhDKARIsAFRNgW_1B1Uv2rMiU0JJ77kX_tuL6kweVxyXImvvrPcTGHUTCXy2aaEfnwIaArV3EALw_wcB
- Логістичний центр. Режим доступу: https://www.roshen.com/pro-roshen/logistychnyy-tsentr

- Mathematical Methods of Modern Statistics 3. Режим доступу: https://conferences.cirm-math.fr/2554.html
- Organizational Modeling. Режим доступу: https://sparxsystems.com/enterprise_architect_user_guide/14.0/guidebooks/tech_ea_organizational_modeling.html
- Маслоутворювач-вотатор Тетра Отич ТВФ-2.06. Режим доступу: https://promf.com/ua/food-equipment-ua/molochne-ua/list-butter-equipment-ua/1375-masloobrazovatel-votator-tetra-otich-tvf-2-06-ua.html
- Датчик температури з перетворювачем сигналу МВТ 3560. Режим доступу: https://ianv.com.ua/category/category-danfoss/promyshlennaya-avtomatika/datchiki-temperaturi/datchik-temperaturi-s-preobrazovatelem-signala-mbt-3560
- Частотний перетворювач GD20-022G-4 (22 кВт). Режим доступу: https://380v.com.ua/ua/product/chastotnii_preobrazovatel4_GD20022G4_22_kvt
- Перетворювач частоти INVT GD200A-011G/015P-4. Режим доступу: https://www.invt.su/product/preobrazovatel-chastoty-invt-gd200a-011g/015p-4.html
- TRT-60LA SSR Solid State Relay 4-20MA to AC Output 28-280V AC AC Solid State Relay Board Voltage Relay. Режим доступу: https://aliexpress.ru/item/33020729592.html?sku_id=67213373392

ДОДАТОК А - ТЕКСТ ПРОГРАМИ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.23001-01 12 01

Листів 6

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп'ютерної системи третього апеляційного адміністративного суду. Програма призначена для

забезпечення налаштування динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и SSH комп’ютерної системи.

ЗМІСТ

•

• Налаштування роутера R2_Anikeev

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2_Anikeev
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.68.0.129 10.68.0.139
!
ip dhcp pool POOL_LAN2
 network 10.68.0.128 255.255.255.128
 default-router 10.68.0.129
 dns-server 10.68.1.85
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local

!
license udi pid CISCO2911/K9 sn FTX1524602K-
```

```
!
no ip domain-lookup
ip domain-name Shchetinin_R1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 description LAN Admin
 ip address 10.68.0.129 255.255.255.128
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
!
interface Serial0/0/1
 description WAN R1
 bandwidth 128
 ip address 10.0.10.2 255.255.255.252
 ip ospf cost 7500
!
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 23
 router-id 15.15.15.15
```

```
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 10.0.10.0 0.0.0.3 area 0
 network 10.68.0.128 0.0.0.127 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
banner motd #123-18 Anikeev. Enter only have key#
!
radius-server host 10.68.0.150 auth-port 1645
radius-server key Anikeev
!
radius server 10.68.0.150
 address ipv4 10.68.0.150 auth-port 1645
!
!
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
!
!
end
```

- Налаштування комутатора Anikeev_Sw4.1

```
!
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Anikeev_Sw4.1
!
```

```
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Shchetynin_SW_Gosp
!
username 12316z_Shchetynin privilege 1 password 7 082048430017061E010803
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 30
```

```
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 40
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 switchport trunk native vlan 100
```

```
 switchport trunk allowed vlan 20,30,40,99
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 20,30,40,99
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 description LAN Menag
 ip address 10.68.0.2 255.255.255.224
!
ip default-gateway 10.68.0.1
!
banner motd 123-18 Anikeev. Enter only have key
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
end
```

ДОДАТОК Б ТАБЛИЦІ МАРШРУТИЗАЦІЇ

Таблиця маршрутизації на R1_Anikeev

```
Shchetynin_R1# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
C       10.0.10.0/30 is directly connected, Serial0/0/1
L       10.0.10.1/32 is directly connected, Serial0/0/1
C       10.0.10.4/30 is directly connected, Serial0/0/0
L       10.0.10.5/32 is directly connected, Serial0/0/0
O       10.0.10.8/30 [110/15000] via 10.0.10.6, 02:51:55, Serial0/0/0
O       10.68.0.0/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.32/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.64/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.96/27 [110/15001] via 10.0.10.6, 02:51:35, Serial0/0/0
O       10.68.0.128/25 [110/7501] via 10.0.10.2, 03:57:06, Serial0/0/1
O       10.68.1.0/26 [110/7501] via 10.0.10.6, 03:57:06, Serial0/0/0
C       10.68.1.64/27 is directly connected, GigabitEthernet0/1
L       10.68.1.65/32 is directly connected, GigabitEthernet0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/15000] via 10.0.10.6, 03:53:53, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Таблиця маршрутизації на R2_Anikeev

```
Shchetynin_R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 12 subnets, 5 masks
C       10.0.10.0/30 is directly connected, Serial0/0/1
L       10.0.10.2/32 is directly connected, Serial0/0/1
O       10.0.10.4/30 [110/15000] via 10.0.10.1, 03:57:56, Serial0/0/1
O       10.0.10.8/30 [110/22500] via 10.0.10.1, 02:52:45, Serial0/0/1
O       10.68.0.0/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.32/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.64/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
O       10.68.0.96/27 [110/22501] via 10.0.10.1, 02:52:25, Serial0/0/1
C       10.68.0.128/25 is directly connected, GigabitEthernet0/0
L       10.68.0.129/32 is directly connected, GigabitEthernet0/0
O       10.68.1.0/26 [110/15001] via 10.0.10.1, 03:57:56, Serial0/0/1
O       10.68.1.64/27 [110/7501] via 10.0.10.1, 03:57:56, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/22500] via 10.0.10.1, 03:54:48, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Таблиця маршрутизації на Anikeev_R3

```
Shchetynin_R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 13 subnets, 5 masks
O       10.0.10.0/30 [110/15000] via 10.0.10.5, 03:58:34, Serial0/0/0
C       10.0.10.4/30 is directly connected, Serial0/0/0
L       10.0.10.6/32 is directly connected, Serial0/0/0
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.10/32 is directly connected, Serial0/0/1
O       10.68.0.0/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.32/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.64/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.96/27 [110/7501] via 10.0.10.9, 02:53:13, Serial0/0/1
O       10.68.0.128/25 [110/15001] via 10.0.10.5, 03:58:24, Serial0/0/0
C       10.68.1.0/26 is directly connected, GigabitEthernet0/1
L       10.68.1.1/32 is directly connected, GigabitEthernet0/1
O       10.68.1.64/27 [110/7501] via 10.0.10.5, 03:58:34, Serial0/0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/27 is directly connected, Serial0/1/0
L       209.165.202.2/32 is directly connected, Serial0/1/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Таблиця маршрутизації на Router_IPS

```
Shchetynin_R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.10.0/30 [110/15064] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.0.10.4/30 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
C       10.0.10.8/30 is directly connected, Serial0/0/1
L       10.0.10.9/32 is directly connected, Serial0/0/1
C       10.68.0.0/27 is directly connected, GigabitEthernet0/1.99
L       10.68.0.1/32 is directly connected, GigabitEthernet0/1.99
C       10.68.0.32/27 is directly connected, GigabitEthernet0/1.20
L       10.68.0.33/32 is directly connected, GigabitEthernet0/1.20
C       10.68.0.64/27 is directly connected, GigabitEthernet0/1.30
L       10.68.0.65/32 is directly connected, GigabitEthernet0/1.30
C       10.68.0.96/27 is directly connected, GigabitEthernet0/1.40
L       10.68.0.97/32 is directly connected, GigabitEthernet0/1.40
O       10.68.0.128/25 [110/15065] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.68.1.0/26 [110/65] via 10.0.10.10, 02:54:02, Serial0/0/1
O       10.68.1.64/27 [110/7565] via 10.0.10.10, 02:54:02, Serial0/0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7564] via 10.0.10.10, 02:54:02, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Таблиця маршрутизації на Anikeev_R0

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

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O       10.0.10.0/30 [110/15064] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.0.10.4/30 [110/7564] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.0.10.8/30 [110/7564] via 209.165.202.2, 02:54:50, Serial0/1/0
O       10.68.0.0/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.32/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.64/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.96/27 [110/7565] via 209.165.202.2, 02:54:30, Serial0/1/0
O       10.68.0.128/25 [110/15065] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.68.1.0/26 [110/65] via 209.165.202.2, 03:54:58, Serial0/1/0
O       10.68.1.64/27 [110/7565] via 209.165.202.2, 03:54:58, Serial0/1/0
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.0/27 is directly connected, GigabitEthernet0/0
L       209.165.200.1/32 is directly connected, GigabitEthernet0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/27 is directly connected, Serial0/1/0
L       209.165.202.1/32 is directly connected, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 209.165.202.2, 03:54:58, Serial0/1/0
```