

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 бакалавра**

Студенту Черкаський Дмитро Андрійович  
(ПІБ)

Академічної групи 123-20ск-1  
(шифр)

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

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

освітній рівень бакалавр  
(назва освітнього рівня)

на тему: “ Компютерна система торгівельної мережі з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі ”

Виконавець: студент 3 курсу, групи 123-20ск-1 \_\_\_\_\_  
(підпис)

Черкаський Д.А.  
(прізвище та ініціали)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинг.	інституційною	
Кваліфікаційної роботи	Доц. Шедловський І.А.			
Розділів:				
Загальна частина	Доц. Шедловський І.А.			
Проектування комп'ютерної мережі	Ас. Бешта Л.В.			
Розробка апаратної частини	Доц. Ткаченко С.М.			
<b>Рецензент</b>				
<b>Нормоконтролер</b>	Проф.Цвіркун Л.І.			

Дніпро  
2023

«ЗАТВЕРДЖУЮ»  
Завідувач кафедри  
Інформаційних технологій та  
комп'ютерної інженерії  
проф. Гнатушенко В.В.

" " \_\_\_\_\_ 2023 р.

**ЗАВДАННЯ**  
**на кваліфікаційну роботу**

бакалавра  
(назва освітньо-кваліфікаційного рівня)

студенту групи 123-20ск-1 Черкаському Дмитру Андрійовичу  
(група) (прізвище, ім'я та по батькові)

Тема кваліфікаційної роботи “ Компютерна система торгівельної мережі з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі ”

затверджена наказом ректора НТУ “Дніпровська політехніка”  
від 16.05.2023р. № 350-с

Розділ	Зміст	Термін виконання
<b>Стан питання та постановка завдання</b>	<i>На основі матеріалів виробничих практик, інших науково-технічних джерел обґрунтувати необхідність модернізації комп'ютерної системи з детальною розробкою комп'ютерної мережі.</i>	<i>15.03.2023 р.</i>
<b>Технічні вимоги до комп'ютерної мережі</b>	<i>На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної мережі.</i>	<i>01.04.2023 р.</i>
<b>Спеціальна частина</b>	<i>Розв'язати завдання з розробки комп'ютерної мережі автоматизованої системи управління дорожнім рухом з опрацюванням побудови та налаштування.</i>	<i>15.05.2023 р.</i>
<b>Графічна частина</b>	<i>Графічні результати розробки системи подати у вигляді рисунків схем таблиць на 10 арк. формату А4.</i>	<i>25.05.2023 р.</i>

Завдання видав, кер. роботи

(підпис)

Доц. Шедловський І.А.

Завдання прийняв до виконання

(підпис)

Черкаський Д.А.

Дата видачі завдання 01.03.2023 р.

Термін подання дипломної роботи до ДЕК 05.06.2023 р.

## РЕФЕРАТ

Пояснювальна записка: 90 с., 16 рис., 7 табл., 1 додаток, 16 джерел.

Об'єкт розробки: комп'ютерна інформаційна система мережевого торговельного підприємства з детальною розробкою корпоративної мережі.

Мета: створення комп'ютерної корпоративної мережі, яка повинна технічно забезпечувати функціонування інформаційної системи мережі роздрібних магазинів з урахуванням особливостей інформаційного середовища.

Розроблена комп'ютерна мережа забезпечує оперативний обмін інформацією з великими швидкостями за рахунок використання сучасного мережевого обладнання.

Компютерна мережа виконана з урахуванням можливостей програмної та технічної модернізації, удосконалення та розширення.

Основні функції:

- збір та збереження інформації;
- автоматизовану обробку і перенапрвлення інформації в базу даних, захист апаратних засобів мережі від несанкціонованого доступу;
- швидко і якісну обробку запитів за відповідними алгоритмами.

Проект мережі виконано відповідно до завдання.

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

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

СИСТЕМА, КОМП'ЮТЕРНА МЕРЕЖА, НАЛАШТУВАННЯ,  
АДРЕСАЦІЯ, МЕРЕЖЕВЕ ОБЛАДНАННЯ, МОДЕЛЬ

## ЗМІСТ

	Перелік умовних позначень, символів, одиниць, скорочень і термінів	6
	Вступ	7
1	Стан питання і постановка завдання	9
	1.1 Загальна характеристика роздрібних торговельних мереж	9
	1.2 Засоби забезпечення функціонування роздрібних торговельних мереж	11
	1.2.1 Інформаційне забезпечення комп'ютерних систем роздрібних мереж	11
	1.2.2 Актуальність систем безпеки та управління доступом	12
	1.3 Галузь застосування комп'ютерної системи	15
	1.4 Характеристика і структура об'єкта впровадження	18
2	Розробка апаратної частини комп'ютерної системи	21
	2.1 Технічні вимоги до комп'ютерної системи	21
	2.1.1 Вимоги до системи в цілому	21
	2.1.1.1 Структура і функціонування системи	21
	2.1.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи	22
	2.1.1.3 Вимоги до надійності	23
	2.1.1.4 Вимоги безпеки	24
	2.1.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи	24
	2.1.1.6 Вимоги до захисту інформації від несанкціонованого доступу	25
	2.1.1.7 Вимоги до патентної чистоти	27
	2.1.1.8 Вимоги до стандартизації й уніфікації	27
	2.1.2 Вимоги до видів забезпечення	28
	2.1.2.1 Інформаційне забезпечення системи	28
	2.1.2.2 Технічне забезпечення системи	28
	2.1.2.3 Вимоги до організаційного забезпечення	29
	2.1.2.4 Вимоги до складу нормативно-технічної документації системи	30
	2.2 Розробка апаратної частини комп'ютерної системи	31
	2.2.1 Організаційна структура підприємства	31
	2.2.2 Розробка структурної схеми комп'ютерної системи	32
	2.2.3 Вибір та характеристики апаратних засобів комп'ютерної мережі	38
	2.2.4 Захист інформації в комп'ютерній системі	46

2.2.4.1	Особливості інформаційної безпеки мережевих операційних систем	46
2.2.4.2	Особливості взаємодії інформаційної системи з мережами загального користування	47
2.2.4.3	Особливості програмного забезпечення автоматизованих робочих місць системи	49
3	Проектування комп'ютерної мережі та розрахунок її налаштувань	51
3.1	Розрахунок адресації комп'ютерної мережі та схеми адресації пристроїв	51
3.2	Розробка моделі та перевірка роботи комп'ютерної системи	56
3.2.1	Базове налаштування конфігурації пристроїв	59
3.3	Налаштування роботи Інтернет	64
3.4	Розрахунок основних характеристик для вихідного трафіку мережі підприємства	65
4	Розробка компонента системи	68
4.1	Аналітичний огляд стану електронної комерції в Україні	68
4.2	Довіра у сфері електронних комунікацій	70
4.3	Аналітичний огляд структури протоколу «Escrow»	73
4.4	Особливості використовуваного протоколу	73
	Висновки	77
	Перелік посилань	78
	Додаток А. Текст програми налаштувань мережі комп'ютерної системи	81

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ**

ОЗП—оперативний запомнюючий пристрій;

КЗ—контрольована зона;

АРМ—автоматизоване робоче місце;

КІСП – комп’ютерна інформаційна система підприємства;

ЛОМ – локальна обчислювальна мережа;

ЦП – цифровий підпис;

## ВСТУП

Роздрібна мережа в цифрі. Якщо звернутися до цифр, то організації бізнесу торгової роздрібною мережі у країнах займають практично весь ринок. Лише близько 4% посідає дрібні магазини чи окремі точки. Решта займають повноцінні мережі з єдиним господарем. Якщо ж звернутися по статистику, то тут лише 20-30% магазинів входять до торгових мереж. Всі інші магазини та точки збуту – це окремі маленькі підприємства. Однак спостереження свідчать, що ця тенденція йде на поліпшення. З кожним роком окремих точок стає дедалі менше, а мережі все зростають.

У такій галузі, що стрімко зростає і змінюється, як торгівля, здатність інформаційної системи (ІС) до розвитку стає необхідною умовою закріплення та швидкого поширення конкурентних технологій у всіх підрозділах торгової мережі. Замова проектна розробка програмного забезпечення дозволяє у тісній взаємодії із замовником створювати індивідуальну версію його ІС, підтримувати її постійне оновлення та розвиток у тих напрямках, які є пріоритетними для замовника.

Специфіка замовних проектів розробки програмного забезпечення така, що вимагає від компанії-розробника постійного відстеження та впровадження у себе нових технологій - як власне розробки програмного забезпечення, так і ведення проектів. В результаті замовник отримує рішення на основі сучасних ІТ, гнучке та модифіковане.

Сховище даних про фінансові та товарні транзакції призначене для інтеграції оперативної інформації з гетерогенних облікових систем, що забезпечують поточну роботу в різних підрозділах торговельної мережі. Дозволяє формувати корпоративну управлінську звітність.

Аналітичне Сховище завдяки інтеграції та спільному обліку розрізнених даних, оперативна робота з якими ведеться у не пов'язаних між собою системах, забезпечує вирішення таких актуальних завдань, як:

- Ведення взаєморозрахунків із постачальниками (облік у різних валютах, щоденна переоцінка)

- Розрахунок собівартості (облікової вартості) товарів
- Ведення корпоративного балансу
- Надання потоку документів-підстав для довідника «Ставки ПДВ за товарами»
- Розрахунок зміни квот товарів для відвантаження зі складу до магазинів на підставі аналізу даних про товари.

Необхідність в автоматизації вважатимуться найбільш характерною ознакою сучасного ділового середовища. Неавтоматизовані процеси споживають дуже багато ресурсів, можуть призводити до збоїв. З ними неможливо охопити нові сегменти ринку та підвищити конкурентоспроможність компанії. Справедливо це і стосовно застарілого програмного обладнання.

Бізнес пов'язаний із постійним пошуком вдалих рішень. Однак часто серед готових продуктів неможливо знайти відповідний за всіма критеріями. Виходом може стати індивідуальна розробка програмного забезпечення для потреб конкретного підприємства або адаптація існуючих рішень під корпоративні завдання.



## **1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ**

### **1.1 Загальна характеристика роздрібних торговельних мереж**

Підприємства роздрібної мережі - це ефективніший спосіб ведення бізнесу у сфері торгівлі, ніж управління кількома окремими магазинами. Плюси від створення торгової мережі Мережа магазинів має безліч позитивних сторін, але з них можна виділити кілька основних: Велика кількість магазинів дозволить своєму господареві краще регулювати асортимент товару, а також знижувати на нього ціну, якщо це необхідно. Ці дві якості є запорукою успішної торгівлі. Бізнес-план роздрібної мережі завжди включає закупівлю великого асортименту товару у великих кількостях. Така оптова закупівля завжди була вигіднішою, з погляду економії на доставці. До того ж, оптовим покупцям часто дають знижки на продукцію. Мережа магазинів завжди має єдине та централізоване управління. Це говорить про те, що всі рішення ухвалюються швидко і чітко, і на найвищому рівні. Плюс, у таких магазинах найчастіше трудяться лише висококваліфіковані фахівці, що виключає безліч проблем у роботі, які є у дрібніших підприємствах. Цілком можливо зменшувати собівартість товару за рахунок того, що немає необхідності постійного пошуку місць збуту, а також у відсутності реклами. Через це кінцева ціна також буде меншою, що, природно, приверне більше покупців. Бізнес-план роздрібної мережі також має враховувати, кожен окремий магазин розташовується у своєму районі, і попит може бути різні товари. Тобто, невелика самостійність у підборі товару для кожної окремої точки єдиної торгової мережі піде лише у плюс всьому підприємству.

Роздрібна торговельна мережа, яка налічує 19 чи більше магазинів, перетворюється на розряд торгової ланцюга. Інакше кажучи, переходить наступну щабель розвитку. Деякі економісти після проведення розрахунків та спостережень дійшли висновку, що найбільш рентабельною буде та мережа, яка включає 21 або більше магазинів.

Структура торгової мережі

Стаціонарна роздрібна мережа - це не просто кілька торгових точок, які впливають з однієї мети. Це кілька самостійних підприємств, кожне з яких розміщується на певній території та призначається для задоволення потреб населення у певному товарі чи послугах. Управління роздрібною мережею – це процес керівництва цілою мережею торгових точок. Суть управління полягає в тому, що директор повинен стежити за якістю послуг, що надаються, а також за наявністю необхідного товару в цих точках, який користується попитом. За потреби потрібно переглядати асортимент, щоб він максимально точно відповідав запитам населення саме у цьому районі.

Асортимент товарів – важлива ознака класифікації підприємств роздрібною торгівлі.

Залежно від виду асортименту розрізняють такі види магазинів:

- Універсальні;
- спеціалізовані;
- магазини із комбінованим асортиментом;
- магазини із змішаним асортиментом товарів.

Універсальні магазини - магазини, що реалізують універсальний асортимент продовольчих та/або непродовольчих товарів. Прикладом універсальних продовольчих магазинів є: універсам, супермаркет, гіпермаркет; універсальних непродовольчих – універмаг, торговий дім.

Спеціалізовані магазини - магазини, що реалізують одну групу товарів ("Одяг", "Культтовари", "М'ясо") або частину товарної групи ("Дитячий одяг", "Спортивні товари", "Ковбаси"). Останніх прийнято називати вузькоспеціалізованими магазинами.

Магазини з комбінованим асортиментом товарів - магазини, що реалізують кілька груп товарів, пов'язаних спільністю попиту («Галантерея-парфумерія», «М'ясо-риба») або покупців, що задовольняють якісь потреби («Господарські товари», «Товари для садівника», «Всі для рукоділля», «Дієта»).

Магазини зі змішаним асортиментом товарів - магазини, що реалізують окремі види продовольчих та непродовольчих товарів. Такими магазинами є нині більшість спеціалізованих магазинів, у яких не дотримується спеціалізація та поряд з основним асортиментом продаються інші товари.

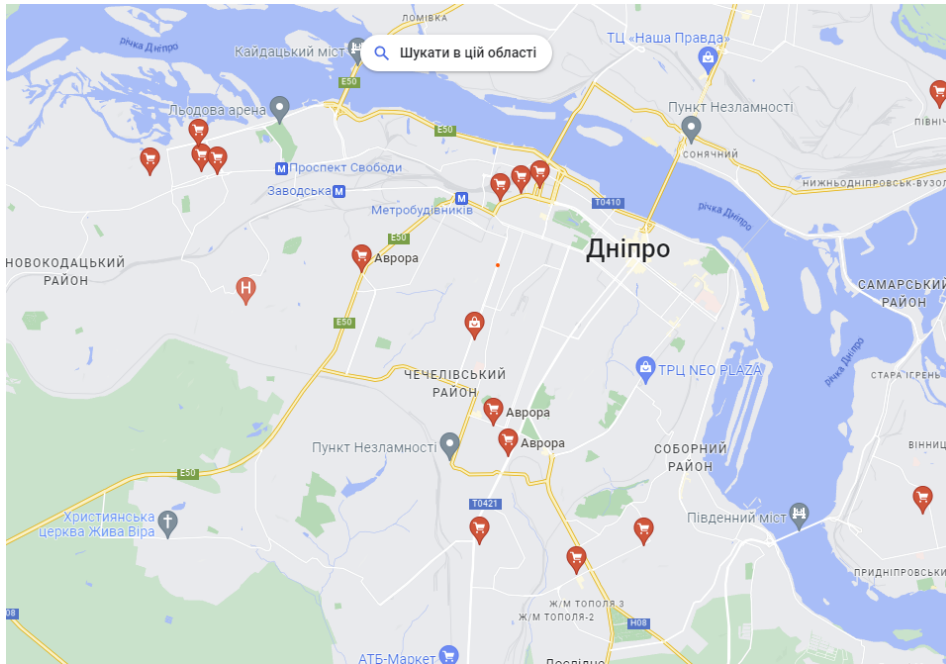


Рисунок 1.1-Мережа магазинів Аврора у м. Дніпро

Аналіз стану роздрібної торгової мережі в Росії показує, що в даний час відбувається процес універсалізації торгових підприємств, зростає кількість змішаних магазинів, кількість яких загалом збільшилася з 9% у 1991 р. до 35% у 1999 р., а в деяких містах - з 1 до 15%. За кордоном також спостерігається тенденція до збільшення кількості великих універсальних магазинів. Це з комплексністю покупок, оскільки покупці прагнуть купувати товари «під одним дахом».



Рисунок 1.2 – Узагальнена схема мережевих торгівельних підприємств.

Число спеціалізованих магазинів помітно скоротилося. Проте спеціалізовані магазини мають низку переваг перед універсальними, комбінованими та змішаними. Вони серйозно працюють з однією товарною групою, що скорочує кількість персоналу та спрощує процес оформлення паперової документації, тісно взаємодіють із постачальниками, забезпечуючи знижки на товари. У перспективі кількість спеціалізованих магазинів має зростати. Особливо це стосується таких магазинів, де реалізуються товари рідкісного попиту: дорогі парфумерно-косметичні товари, модний одяг, вишукані вина.

Додаткові послуги, як і методи продажу товарів, є ще однією складовою форм продажу товарів.Dodatkowe послуги мають велике значення для підвищення культури торгівлі, створення позитивного іміджу підприємства та підвищення його конкурентоспроможності/

Таблиця 1.1 - Класифікація додаткових послуг

<b>Признак класифікації</b>	<b>Характеристика</b>
<b>По часу</b>	
Попередні продажі товарів (допродажні послуги)	Консультація спеціалістів, позамагазинна інформація про товари, демонстрація нових товарів
Під час продажу	Випробування товару у дії, упаковка, дегустація
Післяпродажні	Доставка товарів додому, встановлення куплених виробів вдома у покупців
<b>По ступеню зв'язку з продажем</b>	
Пов'язані з продажем	Додаткова упаковка, консультація про призначення та якість окремих товарів, доставка великогабаритних товарів додому
Відносно пов'язані з продажем	Прикріплення ремінців до годинника, зарядка фотокасет
Вільні	Користування камерою зберігання, виклик таксі, розкрій тканини
<b>По ступеню значущості</b>	
Основні (пов'язані з покупкою) або обов'язкові	Демонстрація товарів у дії, упаковка, консультація спеціалістів
Супутні, додаткові або рекомендовані	Надання розстрочки, короткочасне зберігання товарів
Допоміжні	Довідкове бюро, пошта, театральні каси, ощадні каси
<b>По характеру потреб</b>	
Постійні	Продаж товарів у кредит, кафетерії, телефони-автомати, автомати газованої води
Періодичні	Виставка зразків до свят та попередній прийом замовлень, дегустація кулінарних виробів
Епізодичні	Підбір та відправка товарів на прохання іногородніх покупців
<b>По характеру затрат</b>	
Безоплатні	Підганяння виробів за фігурою покупця, наповнення повітрям гумових іграшок, матраців, кімната матері та дитини
Платні	Гравіювання, ремонт годинників, розтяжка взуття, головних уборів, педикюрний кабінет

Електронний маркетинг - особлива форма прямого маркетингу, що здійснюється за допомогою електронних інформаційних засобів. Включає в себе:

- продаж товарів за телефоном;
- продаж товарів електронними каналами;
- продаж в електронному магазині та ін.

## **1.2 Засоби забезпечення функціонування роздрібних торговельних мереж**

### **1.2.1 Інформаційне забезпечення комп'ютерних систем роздрібних мереж**

Інформаційні системи у оптовій торгівлі грають ключову роль. Без перебільшення можна сказати, що в конкурентній боротьбі перемагають ті організації, які успішніше розвивали свої інформаційні системи, підлаштовуючи їх під потреби клієнтів та внутрішнього обліку.

Починаючи таку велику тему, усвідомлюєш, що однією статтею не обійтися. Розвиток інформаційних систем для оптової торгівлі розпочався 1994 року. З того часу вимоги настільки зросли, що докладний опис кожного розділу вимагатиме окремої статті. А як все добре починалося, досить було зробити невелику програму з єдиною функцією друку витратної накладної. Жодного складського обліку, навіть кошти не треба було враховувати. Потім почалося, що назви кожного товару ліньки набирати, так з'явився довідник номенклатура (товари), далі стало цікаво, що комусь відпускається, з'явився довідник клієнти і сьогодні це довгий список того, що потрібно врахувати, здійснюючи торгові операції, задовольняючи потреби клієнтів.

Озирнувшись крізь роки, видно поступове ускладнення інформаційних систем, для зростаючих потреб оптової торгівлі. В умовах жорсткої конкуренції торгових компаній клієнтам доводиться давати все більше і більше сервісів, наприклад, відстрочка оплати, доставка товару та ін., а це

необхідно відображати в обліку, щоб не забути хто і коли має заплатити гроші.

Окрема проблема ціноутворення. Потрібно акуратно виставити ціни на товари, асортимент безперервно зростає і сягає десятків тисяч найменувань, щоб не торгувати в мінус і мати конкурентноздатні ціни на ринку. Розподілена система складів, безліч розрахункових рахунків, юридичних осіб, присутність у різних регіонах та ще багато проблем, вирішення яких приносить відчутний прибуток, особливо якщо перемогти у конкурентній боротьбі та зайняти значну частку ринку. Але у разі успіху проблеми обліку лише почнуться. Величезна база даних, що містить велику кількість інформації про всю господарську діяльність компанії, вимагає нових підходів. Збитки від простою хоча б на годину вражають, нові вимоги до експлуатації системи посилюються, але їх, принаймні, потрібно сформулювати.

1. Товари та послуги.
2. Покупці.
3. Постачальники.
4. Складський облік.
5. Казначейський облік.
6. Фінансовий облік.
7. Регламентні операції.
8. Управління користувачами.
9. Підтримка користувачів.
10. Експлуатація інформаційної системи.
11. Технічне оснащення.
12. Доопрацювання та розвиток.
13. BtoB.
14. Обмін даними із бухгалтерією.
15. Обмін даними з роздрібною торгівлею.
16. Рекламації.

З цього короткого плану видно, сучасна інформаційна система має безліч напрямів і послуг задля забезпечення торгівлі.

З цього випливає, що картка номенклатури - це складний модуль, який допомагає формувати різні картки товарів із заданими реквізитами. Для зручності введення складних видів даних потрібна можливість формування одних реквізитів залежно від інших. При певних значеннях одних параметрів виникають або зникають з картки товару інші параметри.



Рисунок 1.3 – Централізоване управління торгівельною мережею

При доборі номенклатури в документи або в роздумах купити без фільтра за параметрами заданих для товару не обійтися. Важливо, щоб у картках номенклатури була достовірною і повною, тоді клієнтам буде потрібний товар і відповідно продажу будуть високому рівні.

CRM – термінологічна система, за допомогою якої передбачається покращити стосунки з клієнтами. Потрібно наполегливо добиватися систематизації та повноти інформації про своїх клієнтів. Даних має бути достатньо, щоб при зміні персонального менеджера, який підхопив прапор співробітнику не важко вникнути у справи, поточні продажі, домовленості з



клієнтом. Для цього необхідно акуратно вести та зберігати телефонні дзвінки, електронні листи та інші факти спілкування.

Очевидно, що всі домовленості потрібно ретельно фіксувати в інформаційній системі, клієнти змінять постачальника, якщо їм постійно доведеться нагадувати про досягнуті домовленості. Обіцяли знижку чи хорошу ціну на певний товар, обов'язково потрібно виконати свої обіцянки.

Є регламентні операції, виконувані виключно фахівцями, найпоширеніша їх це контроль помилок у даних. Робота дуже творча, але обов'язково потрібно виявляти та виправляти існуючі в інформаційній системі помилки. Формування набору інструментів залежить від особливостей функціонування створеної системи.

### **1.2.2 Актуальність систем безпеки та управління доступом**

Інформаційною системою користуються багато співробітників організації, позаштатні співробітники, співробітники контрагентів. Створювати та стежити за діями користувачів необхідно адміністратор(у/ам) інформаційної системи. Обмеження доступу до інформації необхідні хоча б з міркувань безпеки та збереження комерційних таємниць.

Звільнення співробітників, прийом нових, зміна прізвищ, все це робота з користувачами системи, хтось цим повинен займатися і робота у нього буде.

Користувачам з обмеженнями прав обов'язково виникають проблеми, які вони самостійно вирішити не можуть, їм потрібна допомога адміністратора. Чим більше обмежень, тим більше запитів надійде від користувачів.

Тестувати програму потрібно не лише від повних прав, а й від обмеженого доступу. Дуже часто ситуація, коли від імені повних прав працює все швидко і без помилок, а з обмеженнями доступу виникає купа помилок та тривалий відгук.

Крім проблем у користувачів виникають питання, пропозиції, питання щодо нових модулів або логіки роботи системи та невпевненість у результаті дій. Будь-яка інформаційна система буде мертвою, якщо ніхто не консулює і не навчає користувачів. Відповідальність за дії в системі висока і мало кому хочеться бути винним, коли не розумієш, що відбувається та які наслідки викличуть дії.

При навчанні важливо показати, як треба робити інакше безвідповідальні нароблять того, чого не варто робити. Небагато уваги людям треба приділити, поки вони не зрозуміють, що нові поля та форми їм не ворог, а дуже корисні алгоритми, що багаторазово підвищують їхню продуктивність праці і дозволяють трохи розслабити мозок, бо все саме розраховується. Надалі користувачі будуть навіть вдячні, незважаючи на те, що спочатку упиралися і не бажали працювати у невідомих джунглях інформації.

#### Експлуатація інформаційної системи

Основний життєвий цикл полягає саме у отриманні інформації із системи. Це верстат переробляє первинні дані і систематизує їх. Умілий аналітик із заготовок зробить чудовий інформаційний продукт із корисними для людства властивостями.

Забезпечення безперебійної роботи 24/7 є складним завданням, але його просто необхідно виконати. При простій інформаційної системи життя в офісі завмирає, не одержуючи потрібної інформації, жоден співробітник не може виконувати свої обов'язки.

До стабільно працюючої системи набагато вищий рівень довіри. Продаж ведеться в максимально швидкі терміни і кожна хвилина на рахунок, повною мірою проявляється фраза: «Час – гроші».

За хорошого обсягу продажів накопичується велика кількість інформації. Історія продажів за багато років є певною цінністю і потрібна в оперативному доступі для аналітиків та інших співробітників організації.

Торгова інформаційна система працює в Hi-Load режимі та вимагає швидкодіючих систем зберігання та обробки даних.

Сервера системи крім надійності повинні мати унікальну швидкодію як апаратних засобів, так і програмного забезпечення.

Світ активно розвивається і торгівлі необхідно постійно змінюватися, покращуючи обслуговування своїх клієнтів, деталізуючи аналітику, надаючи нові сервіси.

«Найкраще – ворог хорошого» діє безвідмовно. Є спокуса нічого не чіпати, начебто й так працює, а після модернізації довго доводиться боротися з помилками та самовіддано їх виправляти.

Там, де є складнощі, є шанс перемогти в конкурентній боротьбі. Ті компанії, які успішно справлятимуться з проблемами модернізації – залишаться на ринку продажу.

### **1.3 Галузь застосування комп'ютерної системи**

Проблема вдосконалення інформаційного забезпечення діяльності в даний час має найважливіше значення для будь-якого суб'єкта господарювання, що функціонує в умовах ринкового середовища.

Для суб'єктів комерційної діяльності проблема вдосконалення інформаційного забезпечення незмірно актуальніша у зв'язку зі швидким зростанням кількості цих суб'єктів, а з урахуванням сфери здійснення комерційної діяльності – у зв'язку з ідентичністю використовуваних торгових технологій, аналогічністю товарів, що реалізуються, однорідністю змісту функціональних процесів комерційної діяльності конкуруючих суб'єктів.

Ринок інформаційних технологій насичений різними інформаційними системами, що включають ІТ-інфраструктуру (комп'ютерне, телекомунікаційне, технологічне обладнання та програмне забезпечення) та ІТ-сервіси, що надаються на її основі. Головне призначення інформаційних систем полягає у забезпеченні єдиного середовища для оперативного управління існуючими обчислювальними комплексами організації, систем

управління базами даних та корпоративним програмним забезпеченням, телекомунікаційним та мережевим обладнанням, пристроями зберігання даних, персональними та мобільними комп'ютерами користувачів, периферійним та технологічним обладнанням.

З усієї безлічі існуючих програмних продуктів нами будуть розглядатися ті, які максимально відповідають змісту комерційної діяльності з урахуванням її видової (торгової) специфіки.

З урахуванням змістовної специфіки комерційної діяльності нам видається виділити як «базових» інформаційних систем такі (таблиця 1.2).

Призначення, завдання та результати використання базових інформаційних систем для комерційної діяльності роздрібною організацією торгівлі.

Таблиця 1.2 - Особливості інформаційного середовища

Наименование информационной системы	Назначение использования	Задачи использования	Результаты использования
MRP – Materials requirements planning (планування потреб у матеріалах)	Стратегічне планування	– задоволення потреб у матеріалах та комплектуючих для планування виробництва споживачеві; - Підтримка необхідних рівнів запасів матеріальних ресурсів, готової продукції; – планування виробничих операцій, розкладів доставок, закупівель	– розрахунок оптимального обсягу партії випуску продукції, що мінімізує суму витрат: - Розрахунок переробки матеріальних ресурсів у готову продукцію (додана вартість, що включає в себе амортизацію обладнання та трудовитрати); - Розрахунок зберігання запасів готової товарної продукції
MRP II – Manufacturing resource planning (планування	Оперативне управління	– оптимальне формування потоку матеріалів (сировини), напівфабрикатів (в т.ч.	- Отримання оперативної інформації про поточні результати діяльності організації в

виробничих ресурсів)		що у виробництві) і готових виробів; - Інтеграція всіх основних процесів, що реалізуються організацією: постачання, запаси, виробництво, продаж та дистрибуція, планування, контроль за виконанням плану, витрати, фінанси, основні засоби і т.д.; – довгострокове, оперативне та детальне планування діяльності організації	цілому і з повною деталізацією на замовлення, види ресурсів, виконання планів; - Коригування планів на основі оперативної інформації; – оптимізація виробничих та матеріальних потоків; - Реальне скорочення матеріальних ресурсів на складах; – реальний вплив на цикл виробництва з метою досягнення оптимальної ефективності виробничих потужностей, всіх видів ресурсів та задоволення потреб замовників; - Повний контроль платежів, відвантаження товарно-матеріальних ресурсів та строків виконання договірних зобов'язань; - Значне скорочення невиробничих витрат; - Окупність інвестицій в інформаційні технології; - Можливість поетапного впровадження системи з урахуванням інвестиційної політики конкретної організації
LP – Lean Production (економне виробництво)	Логістичне управління	– дотримання високих стандартів якості продукції; - зниження виробничих витрат; - Швидке реагування на споживчий попит; – скорочення термінів	– дотримання високих стандартів якості продукції; - зниження виробничих витрат; - Швидке реагування на споживчий попит; – скорочення термінів

		переналадження обладнання	переналадження обладнання
ERP – Enterprise resource planning (планування ресурсів продукції)	Планування ресурсів	<ul style="list-style-type: none"> <li>– оптимізація за часом та ресурсами процесів виробництва та реалізації продукції;</li> <li>– управління фінансовою та господарською діяльністю підприємства;</li> <li>– координація виконання основних операцій та забезпечення повторюваності набору правил та процедур</li> </ul>	<p>Оперативність отримання інформації для прийняття управлінських рішень;</p> <ul style="list-style-type: none"> <li>- Створення інфраструктури електронного обміну даними з постачальниками та споживачами;</li> <li>- Типізація завдань, загальних для підприємств різних видів діяльності;</li> <li>– значну увагу до засобів підтримки прийняття рішень та засобів інтеграції зі сховищами даних;</li> <li>- автоматизація завдань управління бізнес-процесами</li> </ul>
CSRP – Customer Synchronized Resource planning (планування ресурсів підприємства, орієнтоване споживача)	Маркетингове планування та управління	<ul style="list-style-type: none"> <li>– синхронізація потреби покупця з внутрішнім плануванням та виробництвом;</li> <li>– облік споживчих переваг та доданої цінності товару для споживачів;</li> <li>- Формалізація маркетингових методів ведення бізнесу</li> </ul>	<ul style="list-style-type: none"> <li>– забезпечення збалансованості інтересів покупців, постачальників та посередників;</li> <li>– забезпечення цілісності процесу планування шляхом зниження обсягу повторних робіт та кількості перерв через «напливи» замовлень;</li> <li>- Реальний облік фактичного, а не прогнозного попиту;</li> <li>- Доступ у реальному часі до інформації про замовлення покупців;</li> <li>– динамічність зміни послідовності робіт, виконання замовлень, придбання та укладання субконтрактів для покращення обслуговування та</li> </ul>

			зниження вартості готової продукції; – скорочення часу товарних поставок; - Скорочення виробничих витрат; - Організація зворотного зв'язку з покупцями
--	--	--	---

У порядку обґрунтування можливості використання наведених у таблиці інформаційних систем для комерційної діяльності роздрібною організацією торгівлі вважаємо за необхідне дати кілька уточнюючих пояснень.

Виникнення системи MRP було зумовлено завданням автоматизації управління запасами в умовах великосерійного та масового виробництва товарів споживчого призначення та товарної насиченості ринку, які продемонстрували, що використання математичних моделей планування попиту та управління запасами веде до суттєвої економії коштів, «заморожених» у вигляді запасів та незавершеного виробництва.

Але розробити абсолютно оптимальні методи планування запасів неможливо, оскільки алгоритми управління вимагають їхньої адаптації до специфіки конкретних складських завдань залежно від циклу товарного виробництва та поставок, товарної номенклатури запасів, їх вартості, використання під їх зберігання кубатури складів, реалізованого та потенційного попиту тощо.

Значимість практичного вирішення завдання автоматизації управління запасами визначалася положенням у тому, що вибір оптимального розміру партії одна із найважливіших умов підвищення ефективності комерційної діяльності організації, оскільки занижений обсяг товарної партії веде до зростання витрат за управління при повторних замовленнях, а надлишковий – до «заморожування» коштів у товарних запасах.

Тому спочатку автоматизовані системи управління запасами було розроблено для промислового виробництва, ґрунтувалися на розрахунках за

специфікацією складу виробу. За планом випуску продукції формувалися плани виробництва та розраховувався обсяг закупівлі матеріалів та комплектуючих виробів.

Першою інформаційною системою, що забезпечує автоматизоване вирішення названого завдання, стала система MRP, основною відмінністю якої від математичних моделей управління запасами, що передбачають незалежний попит на всю товарну номенклатуру, став розрахунок запасів для номенклатури «залежного», що визначається потребами ринку (попиту), що оформляється замовленням на готову товарну продукцію.

#### Інфраструктура моделі MRP

Система MRP використовує як «вступні» прогнози обсяги продажів, рахунки-фактури на поставку матеріалів та документи по господарських операціях у розрізі окремих продуктів, а також дані щодо балансових залишків по кожному виду сировини, матеріалів, що комплектують для моделювання взаємозалежності періодичності замовлень на поставку матеріальних оборотних ресурсів та виробничого графіка.

Виробнича потреба зіставляється з поточним залишком видів сировини та матеріалів, у разі потреби дозакупівлі яких система MRP оцінює логістичний цикл (іноді від моменту замовлення до надходження партії матеріалів на склад організації) та виводить тимчасовий графік закупівель, щоденну потребу у розрізі видів сировини та матеріалів.

Практика використання MRP системи виявила притаманні їй недоліки: значний обсяг обчислень та попередньої обробки даних; зростання логістичних витрат на обробку замовлень та їхнє транспортування, що породжується прагненням організації зменшити запаси матеріальних ресурсів, реконструювати виробництво на випуск малих обсягів товарної продукції з високою частотою виконання замовлень; нечутливість до короткочасних змін попиту; велика кількість відмов через велику розмірність системи та її комплексність; недостатньо точне відстеження попиту та



обов'язкова наявність страхових запасів, що «заморожують» оборотні кошти організації.

Перелічені недоліки спричинили створення системи MRP II, що володіє більшою гнучкістю планування, що забезпечує кращу організацію поставок і більш швидку реакцію зміну попиту.

Класична система MRP II складається з 16 основних функціональних блоків (підсистем та модулів): планування продажу та виробництва, управління попитом, складання плану виробництва, планування матеріальних потреб, специфікація продуктів, управління запасами та складськими операціями, планові поставки, управління на рівні виробничого цеху, планування виробничих потужностей, контроль входу/виходу, матеріально-технічне постачання, планування ресурсів розподілу, планування та контроль виробничих операцій, управління фінансами, моделювання, оцінка результатів діяльності.

В основу системи MRP II покладено ієрархію планів: план вищого рівня надає вхідні дані, намічені показники та (або) будь-які обмежувальні умови для планів нижчого рівня. Між планами вищого та нижчого рівнів існує зворотний зв'язок. Якщо результати плану нереалістичні, система передбачає можливість їх перегляду. Таким чином, система MRP II дозволяє координувати попит та пропозицію ресурсів на всіх рівнях планування діяльності організації.

Інформаційні системи MRP та MRP II отримали свій розвиток у логістичній інформаційній системі LP, заснованій на принципі постачання JiT («точно в термін»), концепції TQM (Total Quality Management – загальне управління якістю) та серії стандартів системи управління якістю ISO-9000.

Ще однією інформаційною системою, визначеною нами як «базову» для комерційної діяльності організації, є система ERP, що включає: управління ланцюжком поставок; удосконалення планування та складання розкладів; модуль автоматизації продажу; автономний модуль, який відповідає за конфігурування; остаточне планування ресурсів; технології

оперативного аналізу даних у реальному часі; модуль електронної комерції; керування даними про виріб.

Система ERP забезпечує можливість автоматизації всіх ключових аспектів діяльності організації: виробництво, планування, фінанси та бухгалтерія, матеріально-технічне постачання, управління кадрами, збут, управління запасами, ведення замовлень на виготовлення (постачання) продукції та надання послуг.

Головними відмінностями системи ERP від систем MRP та MRP II є:

- більша увага фінансовим підсистемам, а отже, більша відповідність цільовому призначенню комерційної діяльності – одержанню прибутку;

- орієнтованість на управління «віртуальним» підприємством, що відображає взаємодію виробництва, постачальників, партнерів та споживачів, а отже, більша відповідність завданням комерційної діяльності;

- доповнення механізмами управління транснаціональними корпораціями, включаючи підтримку кількох часових поясів, мов, валют, систем бухгалтерського обліку та звітності, а отже, забезпечення стандартизованості комерційної діяльності та можливості здійснення електронної комерції.

Завершальною «базовою» інформаційною системою комерційної діяльності організації є система CSRP, що використовує інтегровану функціональність системи ERP і перенаправляє виробниче планування від виробництва до покупця з метою створення продуктів із підвищеною (доданою) цінністю для останнього.

У цій системі інформація від покупців надходить до підрозділів організації з чотирьох основних функціональних напрямків: продаж та маркетинг; обслуговування покупців; технічне обслуговування; дослідження та розробки.

Таким чином, система CSRP інтегрує діяльність організації, з яскраво вираженою орієнтацією на покупця, ставить цю орієнтацію в центр усієї

системи управління бізнесом, що повністю відповідає змістовній специфіці комерційної діяльності.

#### **1.4 Характеристика і структура об'єкта впровадження**

Зауважимо, що «базові» інформаційні системи, що виділяються нами, і розкриті їх основні характеристики дозволяють зробити висновок про можливість їх використання в процесі комерційної діяльності організації.

Однак якщо перші дві з розглянутих систем (MRP та MRP II) більш прийнятні для організацій-товаровиробників, самостійно, без участі торгових посередників, що реалізують продукцію на споживчому ринку, то три наступні системи (LP, ERP, CSRP) – одночасно і для організацій-товаровиробників, й у торгових посередників – учасників логістичної системи руху товарної продукції від виробника до споживача.

#### **Висновки**

Метою кваліфікаційної роботи є створення проекту обчислювальної мережі для автоматизованої системи управління процесом продажів торгівельною мережею.

Відповідно до завдання комп'ютерна мережа повинна забезпечувати ефективну роботу системи і мати можливість до розширення своїх функціональних можливостей.

Для зв'язку локальних робочих станцій мережі з сервером доцільно використовувати Ethernet з гігабітними швидкостями передачі даних.

Виходячи з характеристик мережі доріг міста, його площі і відстаней доцільно використовувати стандарт 1000BASE-T.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ**

### **2.1 Технічні вимоги до комп'ютерної системи**

#### **2.1.1 Вимоги до системи в цілому**

##### **2.1.1.1 Структура і функціонування системи**

Основне призначення інформаційної системи – забезпечення високоефективної роботи підприємства.

Структурно система складається з головного офісу та мережі торгових підрозділів.

Кожен із підрозділів обладнано системами відеоспостереження, контролю доступу, контролю наявності товарів, контролю плинних показників діяльності.

Вимоги до функцій інформаційної системи:

Функції, що виконуються системою, поділяються на такі групи:

інформаційні;

керуючі;

функції забезпечення торгівлі.

Інформаційні функції включають:

збір та первинну обробку даних;

реєстрацію поточних подій;

реєстрацію аварійних подій;

архівацію, зберігання та надання ретроспективної інформації;

забезпечення можливості аналізу дії;

можливість обміну інформацією із суміжними системами за протоколом обміну.

Керуючі функції повинні забезпечувати:

подання керуючих директив;

дистанційне керування та контроль.

Функції захисту:

діагностику та видачу повідомлень щодо відмов елементів комплексу технічних засобів;

автоматичне відключення з метою забезпечення захисту даних та обладнання;

збір та обробку інформації;

управління сигналізацією та оповіщенням.

### **2.1.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи**

Регламент обслуговування визначається паспортами чи експлуатаційною документацією на компоненти системи.

Періодичність резервного копіювання баз даних має бути відображена в експлуатаційній документації.

Для забезпечення регламенту обслуговування програмні засоби контролю стану технічних засобів повинні забезпечувати контроль, діагностику та тестування для виявлення та локалізації несправностей у технічних засобах у процесі функціонування (без порушення працездатності комплексів) з можливістю відображення стану технічних засобів.

Чисельність обслуговуючого персоналу має бути достатньо ефективного виконання персоналом покладених нею обов'язків з експлуатації Системи. Забезпечення повинно включати вимоги щодо чисельності та кваліфікації персоналу, інструкції щодо кожного виду діяльності, та точне визначення виконуваних функцій.

Інструкції для персоналу повинні визначати його дії під час експлуатації як у нормальному режимі, так і за відмов технічних засобів.

Комп'ютерна система повинна забезпечувати повноцінне функціонування підприємства.

Загальна кількість робочих місць – не менше 90. Режим роботи комп'ютерної системи – цілодобово.

Структура мережі повинна складатися з п'яти під мереж LAN1 – LAN5.

Кількість вузлів: LAN1 – 45 LAN2 – 12 LAN3 – 25 LAN4 – 6 LAN5 – 8.

Інтенсивність трафіку  $\mu = 85$  (кадрів/с).

Блок адрес - 172.23.IPn.0/21; для виділення підмереж IPn = 224.

Зовнішня адреса сервера HTTP: 209.165.200.4.

Середня тривалість вихідного повідомлення у найбільшій мережі – 600 байт.

Затримка передачі пакету у найбільшій мережі –  $\leq 5$  мс.

### **2.1.1.3 Вимоги до надійності**

Інформаційна система має забезпечувати такі значення показників надійності виконання основних функцій:

режим роботи – безперервний (24ч/добу);

середнє напрацювання на відмову з інформаційних функцій – не менше 40 000 год;

середнє напрацювання на відмову за функціями управління – не менше 50 000 год;

середнє напрацювання на відмову у функціях захисту – не менше 120 000 год;

середній час відновлення працездатності системи за будь-якою з функцій, що виконуються, не повинен перевищувати 60 хв;

коефіцієнт готовності системи за основними функціями – не менше 0,99;

середній час відновлення після збою із заміною модулів із ЗІП – не більше 1 години;

термін служби має становити щонайменше 15 років.

### **2.1.1.4 Вимоги безпеки**

Умови безпеки роботи персоналу з експлуатації обладнання інформаційної системи мають відповідати існуючим тренуванням та нормам.

Додатково необхідно передбачити:

Передбачити можливість електроживлення ІС від двох незалежних введів через одне джерело безперебійного живлення, яке має можливість автоматичного вмикання резерву;

Передбачити безперебійне електроживлення з роботою в автономному режимі не менше 4-х годин та байпасом.

Живлення апаратних засобів (верхнього рівня) та контролерів повинно здійснюватися від окремих джерел безперебійного живлення ДБЖ з тимчасовим збереженням працездатності не менше 480 хвилин при зникненні електроживлення на вході.

#### **2.1.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи**

Система повинна забезпечувати роботу об'єкта, незалежно від його режиму роботи, для безперервних процесів – у цілодобовому режимі.

Функції централізованого контролю поточних значень параметрів повинні виконуватися безперервно, а також комбінованому режимі, що поєднує операції контролю стану, що проводяться безперервно, і відносно рідкісні операції управління, що виконуються Системою на запит адміністратора.

Для окремих підрозділів, оснащених локальними системами, має бути передбачено можливість дистанційного режиму управління.

Система (в цілому) та її основні компоненти (підсистеми, комплекси засобів) повинні функціонувати в режимі, що обслуговується, що передбачає можливість екстреного обслуговування (наприклад, заміни елемента, що відмовив) і мінімально необхідний обсяг операцій з планового (штатного) експлуатаційного обслуговування.

При появі позаштатних ситуацій (відключення зовнішнього живлення, збій у системах введення-виведення та інше) у Системі мають бути реалізовані алгоритми управління, спрямовані на переведення обладнання у безпечний стан.

Як запасні резервні елементи системи дистрибутив програмного забезпечення повинен зберігатися на зовнішніх носіях з інструкцією та програмою інсталяції.

Склад ЗІП визначається на етапі проектування відповідно до технічних вимог щодо надійності та обсягу фінансування проекту і повинен включати від 20% до 40% всіх компонентів системи (модулі, процесори, HDD, комутатори, бар'єри та ін.).

#### **2.1.1.6 Вимоги до захисту інформації від несанкціонованого доступу**

Програмне забезпечення має бути захищене від несанкціонованого доступу:

стандартними засобами безпеки, що надаються операційною системою;  
стандартними засобами системи ERP (ідентифікація/автентифікація користувачів та розмежування прав доступу).

Повинен забезпечувати контроль рівнів доступу користувачів до різних груп операцій, які мають поділятися на групи:

адміністрування системи (редагування екранів процесу, конфігурування системи);

оперативне управління;

робота із системою захисту.

По кожній групі можуть бути забезпечені такі рівні прав доступу:

"Перегляд" - тільки перегляд;

"Управління" - дозволено управління;

«Інженер» – дозволено зміну налаштувань;

«Системний адміністратор» – дозволено всі операції, у тому числі зміну прав інших користувачів.

#### **2.1.1.7 Вимоги до патентної чистоти**

В комп'ютерній системі повинні використовуватися елементи та пристрої, програмне забезпечення ліцензовані та сертифіковані для



використання на території України.

### **2.1.1.8 Вимоги до стандартизації й уніфікації**

Стандарти та універсальність обладнання повинно бути узгоджено:

- Великоблочне обладнання.
- Каналоутворювальне обладнання зв'язку та обладнання електроживлення.

Обладнання та матеріали, що поставляються, повинні мати:

- дозвіл на застосування конкретних видів (типів) технічних пристроїв на виробничих об'єктах.
- сертифікати відповідності вимогам промислової та пожежної безпеки;
- необхідну технічну документацію, а саме:
  - заводські паспорти обладнання;
  - інструкції заводу-виробника з ремонту, технічного обслуговування, експлуатації та монтажу обладнання;
  - технологічні та монтажні схеми приєднання та монтажу.

### **2.1.2 Вимоги до видів забезпечення**

#### **2.1.2.1 Інформаційне забезпечення системи**

Програмне забезпечення має будуватися як децентралізований програмний комплекс, у якому програми та дані розподілені між різними рівнями управління та реалізований за модульним принципом.

Усі програмні засоби, що поставляються у складі ПТК, повинні мати ліцензійні угоди (ліцензії), що підтверджують правомочність їх використання. ПЗ має поставлятися з діючими комплектами ліцензій, що відповідають числу робочих місць або тегів, на яких його передбачається встановлювати, та мати пізнішу за часом випуску версію виробника. Необхідно передбачати можливість відновлення ліцензій у разі несправності

системи та можливість централізованого динамічного управління та розподілу по системах\підсистем без застосування твердих ключів.

Програмні засоби, що застосовуються, повинні відповідати наступним умовам:

- бути офіційною версією розробника/вендора;
- мати офіційне підтвердження сумісності (прикладних систем із загальносистемним ПЗ та навпаки, включаючи нові версії ПЗ) від розробника/вендора, або мати документально підтверджений висновок про успішні випробування;

- відповідати вимогам щодо ліцензійної чистоти, не порушувати чийсь права інтелектуальної власності;

- мати комплект експлуатаційної документації, включаючи посібники адміністраторів та користувачів (операторів) українською мовою.

ПЗ повинно мати такі характеристики:

- виконувати весь перелік налаштованих користувачем прикладних програм та алгоритмів управління та захисту;

- збої у роботі програм, відмови частини обчислювальних засобів, помилки персоналу повинні діагностуватися, супроводжуватися повідомленнями;

- система повідомленні повинна мати інтерфейс для статистичного аналізу подій за певний період з можливістю фільтрації за типами подій та порівняння з попередніми періодами;

- система повідомлень повинна мати інтеграційний інтерфейс для сторонніх систем автоматичної обробки даних і підтримувати вивантаження інформації у стандартних форматах (CSV, XLSX).

- Забезпечувати можливість автоматичного перезапуску при відновленні електричного живлення після його відключення;

- мати можливість оперативного конфігурування у процесі функціонування;

- мати можливість модифікації та перезавантаження в режимі on-line, без зупинки технологічного процесу.

Засоби розробки прикладного програмного забезпечення повинні давати можливість реалізувати проектні методи регулювання та управління технологічним процесом. Прикладне ПЗ повинно забезпечувати глобальний пошук конфігурації модулів, блоків та параметрів блоків.

Повинна бути передбачена різна функціональність та різні групи тривожних сигналів, структурування системи оповіщення тривожними сигналами з прив'язкою до робочих станцій, розподілена система ведення журналів подій та накопичення історичних трендів, зручні та інтуїтивно зрозумілі засоби редагування конфігурації з використанням стандартних програм Windows ( .

Повинні підтримуватися засоби розробки відеокадрів з використанням стандартних, розширених і користувацьких бібліотек графічних елементів, повинна бути вбудована підтримка у відеокадрах скриптів користувача, групування графічних елементів у складні об'єкти, підтримуватися динамічна анімація елементів зі зміни значень параметрів, можливості використання HTML5 .

Програмне забезпечення, що застосовується, повинно відповідати наступним загальним вимогам:

- централізація – основу системи має становити єдина база даних, яка дозволить охопити всі виробничі процеси;
- розширюваність і масштабованість - програмне забезпечення, що використовується, повинно забезпечувати збільшення продуктивності при збільшенні потужності апаратних серверних ресурсів;
- відкритість – організація двосторонньої взаємодії з іншими автоматизованими системами, що забезпечується застосуванням сучасні стандарти доступу до даних (ODBC, OLE DB, OPC DA, OPC UA (клієнт/сервер), HDA, OPC Xi). Забезпечення необхідної інтеграції з діючими

та інформаційними системами, що функціонують на підприємстві, включаючи підтримку MQTT протоколів;

- захист інформації – високий рівень захисту інформації на основі багаторівневої системи контролю доступу, ведення протоколів дій користувачів та всіх змін, що вносяться в систему, шифрування протоколів на основі TLS методу;

- живучість - виконання покладених функцій у повному або частковому об'ємах при збоях та відмови, відновлення після збоїв;

- гнучкість системи – адаптивність до змін у процесах, системах автоматизації, бізнес-процесах для підприємства;

- індивідуальний підхід та зручність застосування – подання інформації кожному фахівцю підприємства у вигляді технологічних даних та звітів.

### **2.1.2.2 Технічне забезпечення системи**

*Технічні засоби для використання у системі;*

Кабельні лінії повинні відповідати вимогам, встановленим міжнародними стандартами EIA/TIA для комунікаційних ліній у структурованих системах зв'язку.

Кабелі комунікаційних систем мають бути обрані так, щоб їх характеристики відповідали вимогам.

Взаємодія між компонентами контролерного та системного рівнів повинна здійснюватися з використанням протоколу канального рівня Ethernet, протоколу мережного рівня IP та протоколу транспортного рівня TCP по лініях кабельного зв'язку (ВОЛЗ, Мідний кабель передачі даних промислового виконання).

Новий сегмент мережі управління, що забезпечує обмін даними між системами, повинен бути повністю резервованим. Передбачити поетапне введення об'єктів в експлуатацію з мінімальним впливом на діючі системи. Все мережеве обладнання має бути у промисловому виконанні, що враховує умови навколишнього середовища, що ізолює обладнання від впливу

шкідливих факторів навколишнього середовища. Металеві частини інтерфейсів портів RJ-45 повинні бути захищені від впливу руйнівних факторів заглушками та ковпачками. Мережеве обладнання має бути на базі КТС одного вендора з ПЛК та забезпечувати взаємодію по мережі Profinet.

Для підключення кабельних ліній Ethernet CAT6 і CAT7 всередині шафи передбачати проміжні модульні розетки CAT6 для підключення мідних кабельних ліній. Монтаж розеток повинен виконуватися на DIN рейку.

Для підключення оптичних кабельних ліній використовувати оптичні патч-панелі, що монтуються на DIN-рейку. Для кожної оптичної кабельної лінії має бути передбачена окрема патч-панель.

Електропостачання шафового обладнання повинне здійснюватися за окремими лініями: перша лінія від шафи розподілу гарантованого електроживлення, друга від мережі нестабілізованого електроживлення 220V AC.

Розміщення шафового обладнання (що розміщується не в спеціальних приміщеннях) необхідно виконувати в зонах, що виключають затоплення та переважно повинно виконуватися на спеціальних майданчиках у районі основних маршрутів пересування технологічного персоналу.

### **2.1.2.3 Вимоги до організаційного забезпечення**

План щодо забезпечення роботи системи повинен містити наступні етапи:

- 1) дослідження роботи організації та взаємозв'язку її ресурсів;
- 2) оцінка вразливості організації у всіх галузях, включаючи методи роботи, робочий простір та обладнання, збереження та справжність даних, на випадок надзвичайних обставин;
- 3) дослідження впливу можливої аварії на різні рівні роботи організації;

4) бізнес-процес та покроковий опис заходів організаційного забезпечення;

5) розробка короткострокового плану відновлення після аварії;

6) розробка довгострокового плану відновлення після аварії, включаючи план повернення до нормальних ділових операцій та визначення пріоритетів серед функцій, що відновлюються.

У плані забезпечення відмовостійкості системи повинні бути розроблені та визначені:

1) визначено сфери відповідальності;

2) регламент дій у разі аварії;

3) підготовлені шаблони повідомлень, їх ранжування та процедура розсилки;

4) перелік сценаріїв збою;

5) визначено критерії позаштатної ситуації/аварії/аварії;

6) правила відключення/невідключення автоматизованих систем;

7) списки заходів щодо відновлення із резервних копій ОЗ;

8) списки заходів щодо відновлення із резервних копій СУБД;

9) роботи з відновлення прикладного ПЗ;

10) розроблено процеси відновлення даних (дії в умовах аварії, повідомлення, відновлення систем, відновлення даних, оголошення аварії, відновлення мережі, відновлення робочого місця користувача).

#### **2.1.2.4 Вимоги до складу нормативно-технічної документації системи**

Документація на інформаційну систему має включати розробку:

- технічного завдання;

- Завдань на суміжні частини проекту;

- ескізного проекту;

- технічний проект;

- Робочої документації;
- Кошторисної документації.

На етапі проектування мають бути розроблені:

- Стадії "Обстеження", "Технічне завдання":
- Звіт про обстеження у погодженому із Замовником вигляді;
- Технічне завдання;
- завдання на суміжні частини проекту (попередня редакція);
- Стадія "Ескізний проект":
- Ескізний проект
- Стадія "Технічний проект":
- Технічний проект
- Стадія «Робоча документація»:
  - «Загальносистемні рішення»
  - "Технічне забезпечення";
  - «Організаційне забезпечення»
  - «Математичне забезпечення»
  - «Інформаційне забезпечення» у складі:
    - перелік вхідних сигналів та даних;
    - перелік вихідних сигналів та документів;
    - опис систем класифікації та кодування;
    - "Кошторисна документація";
    - «Технічна документація» (попередня редакція);

Стадія «Реалізація»:

- "Інформаційне забезпечення";
- "Експлуатаційна документація";
- "Програмне забезпечення";
- "Виконавча документація";
- «Технічна документація на обладнання та ПЗ»;

На всіх стадіях виконання робіт повинна розроблятися, деталізуватися та актуалізуватися документація, необхідна для організації робіт за проектом (протоколи, графіки виконання робіт, акти тощо).



## **2.2 Розробка апаратної частини комп'ютерної системи**

### **2.2.1 Організаційна структура підприємства**

Вважаємо, що з урахуванням видової специфіки комерційної діяльності її суб'єкти зможуть на основі виділеного нами призначення, завдань, результатів використання інформаційних систем обрати оптимальну з них відповідно до конкретних завдань комерційної діяльності.

Головною перевагою цієї системи, якщо виходити із завдання оцінки можливості її використання у процесі комерційної діяльності організації, є чітка визначеність умов вибору постачальників. Ці умови полягають у наступному:

- Доставка ресурсів повинна здійснюватися відповідно до принципу «точно в строк»;
- ресурси мають відповідати всім стандартам якості, вхідний контроль ресурсів має бути виключений;
- ціни на ресурси повинні бути обґрунтованими, виходячи з орієнтації на довгострокові господарські зв'язки з постачальниками, але при цьому зниження цін має здійснюватися без шкоди якості ресурсів, що поставляються;
- Продавці ресурсів повинні попередньо узгоджувати проблеми і труднощі поставки зі споживачем ресурсів;
- продавці ресурсів повинні супроводжувати їх постачання сертифікатами, що підтверджують контроль якості виготовлення ресурсів;
- Продавці ресурсів повинні сприяти покупцям ресурсів у проведенні експертиз або адаптації технологій до нових модифікацій ресурсів.



Рисунок 2.1 – Організаційно-функціональна структура інформаційної системи.

Автоматизовані системи управління запасами стали охоплювати і сферу реалізації товарної продукції, а сфера їх застосування розширилася до комплексного вирішення виробничих, постачальницьких та збутових завдань діяльності організації, що дозволяло оперативно коригувати планові завдання у процесі виробництва за зміни потреб ринку (попиту).

### 2.2.2 Розробка структурної схеми комп'ютерної системи

Відповідно до характеристик та відстані між об'єктами підприємства в межах міста розробимо схему комп'ютерної мережі [17].

На структурній схемі (Рис. 2.2 ) зображено компютерну мережу яка складається з 5 локальних мереж.

LAN1 – локальна мережа, яка об'єднує підрозділи з підключенням 45 терміналів.

LAN2 – локальна мережа, яка об'єднує 12.

LAN3 – об'єднує 25 терміналів центрального офісу та складу.

LAN4 – локальна мережа яка об'єднує 6.

LAN5 – локальна мережа, яка об'єднує 8.

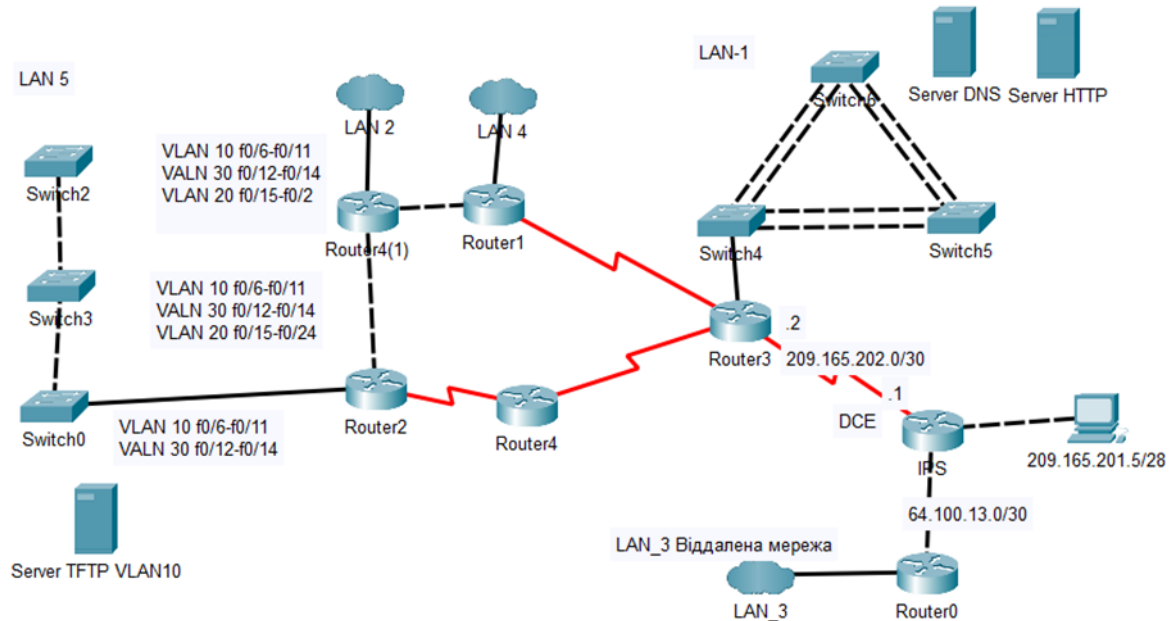


Рисунок 2.2 – Структура комп'ютерної мережі

### 2.2.3 Вибір та характеристики апаратних засобів комп'ютерної мережі

Інтелектуальні та гнучкі мережеві комутатори серії Cisco Catalyst – провідний продукт серед комутаторів усіх рівнів, що характеризується фіксованою конфігурацією, широкою лінійкою моделей для вирішення питань, пов'язаних із забезпеченням коректної роботи локальних мереж.

Мережеві комутатори Cisco Catalyst дозволяють максимально спростити експлуатацію ІТ-інфраструктури, гарантують безпеку бізнес-процесів, забезпечують безперебійне функціонування мережі. Пристрої Cisco Catalyst надають своїм користувачам можливість працювати в так званих

мережах без кордонів. Залежно від серії Cisco Catalyst (2960, 3560, 3650, 3850, 4900, 6500 тощо) визначається призначення комутатора. Це може бути реалізація розширених сервісів у локальних мережах малих, середніх та великих підприємств, а також у мережах філій.

До переваг мережних комутаторів Cisco можна віднести: високий рівень обслуговування користувачів, просте мережеве управління, висока швидкість функціонування мережі (чудова пропускна здатність, тривала автоматизована робота, швидке розгортання), скорочення споживання електроенергії через енергозберігаючу конструкцію, здатність працювати роками без збоїв.

PoE+ комутатор Cisco Catalyst WS-C3750X-48PF-L 2+ рівня, 48 портів 10/100/1000 Мбіт/с. LAN Base. Підтримує сервісні модулі на 4 x 1Гб, 2 x 10 Гб, 2 мідні 10GB, 2x 10 Гб SFP+ Uplinks портів.



Рисунок 2.3 – Вигляд комутатора моделі WS-C3750X-48PF-L Cisco Catalyst PoE+

Серія Cisco Catalyst 3750-X

Тип комутатора Керований

Рівень комутатора 2+ рівень

Тип Cisco IOS

LAN Base

Порти доступу Ethernet 48 x GE RJ-45

Порти агрегації Ethernet

Слот мережевого модуля

Таблиця MAC адрес 32000 MAC адрес  
 Максимальний VLAN ID 4096  
 Стекування StackWise Plus/9  
 Число активних VLAN 1005 VLAN  
 Протоколи VLAN Port-based/802.1Q  
 Габаритні розміри (ВхШхГ) см 44.5 x 4.45 x 49.5 см  
 Пам'ять FLASH 64 Мб  
 Об'єм ОЗУ 256 Мб  
 Робота в кластері Так  
 Потужність номінальна/максимальна 49 Ватт  
 Тип живлення Внутрішній блок 100-240В АС, 50-60 Гц  
 Висота RM UNIT 1U  
 Комутація Мпакетів/с (MPPS) 101,2 MPPS  
 Матриця комутації 160 Гбіт/с  
 Тип установки Стійкове  
 Порти консольні 2 CON  
 Порти живлення PoE 48 PoE+  
 Потужність PoE 800 Вт  
 GTIN/EAN 0854587039621

LAN маршрутизатори призначені для маршрутизації пакетів у локальній мережі, а також її організації та підключення до Інтернету за допомогою портів WAN. Також на базі даних пристроїв можуть бути розгорнуті різні послуги.

#### Основні особливості

Cisco є світовим лідером у сфері виробництва мережного обладнання. Пристрої цієї торгової марки відрізняються великим функціоналом, високою якістю виконання та надійністю своєї роботи. До основних особливостей LAN маршрутизаторів Cisco можна віднести:

Високий рівень продуктивності. LAN маршрутизатори Cisco забезпечують високий рівень продуктивності за рахунок використання пакету послуг QoS, списків доступу (ACL) та технології Performance Routing. Крім того, системні адміністратори можуть додатково впровадити послуги Cisco Wide Area Application Services для застосування вдосконалених методів оптимізації WAN (оптимізація TCP, кешування, стиснення та прискорення роботи програм).

Енергоефективність. LAN маршрутизатори Cisco підтримують інтелектуальне керування живленням, надаючи можливості налаштування потужності кожного з модулів.

керування. За допомогою таких функцій, як IP SLA, Embedded Event Manager та NetFlow, системні адміністратори можуть керувати маршрутизаторами (у тому числі віддалено).

розширення. Системні адміністратори можуть оновлювати карти операційної та флеш-пам'яті для прискорення швидкодії робочих процесів та впровадження додаткового програмного забезпечення.

модульна архітектура Таке рішення передбачає розширення кількості підключень та послуг. У разі можливого оновлення технологій, заміни вимагають лише окремі модулі, а не ціла платформа.

безперервність робочих процесів. Деякі LAN маршрутизатори підтримують стандарти бездротового Інтернету 3G. Завдяки цій особливості у разі обриву з'єднання з основним провайдером гарантується безперервність підключення до Інтернету.

підтримка PoE на портах. Підтримка на портах технології PoE/PoE+ забезпечує живлення по Ethernet-кабелю для обладнання, що підключається.

послуги IP телефонії. Підтримка Cisco Unified Communications Manager Express забезпечує широкий спектр послуг для розгортання IP телефонії.

#### Критерії вибору

При виборі LAN маршрутизаторів рекомендують звертати увагу на значення наступних показників:

кількість портів. Цей показник визначає кількість пристроїв, які підключаються до глобальної мережі. Ви можете вибрати маршрутизатори із підтримкою стандартів Fast Ethernet або Gigabit Ethernet.

слоти для встановлення інтерфейсних карток. Слоти для встановлення інтерфейсних карток забезпечують підвищення ефективності апаратного та програмного забезпечення LAN маршрутизаторів.

обсяг флеш-пам'яті. Цей показник впливає кількість впроваджуваного ПЗ для LAN маршрутизаторів.

обсяг операційної пам'яті. Великий обсяг операційної пам'яті забезпечує швидкодію обробки пакетів даних.

внутрішні сервісні слоти. Зазначений тип слотів призначений для впровадження додаткових послуг за допомогою установки відповідного типу модулів.

мережеві слоти. Ці слоти використовуються для встановлення модулів розширення з портами LAN/WAN.

порти USB. Цей тип портів використовується для встановлення знімних накопичувачів пам'яті, з метою запису різних програм та кількох образів програмного забезпечення.

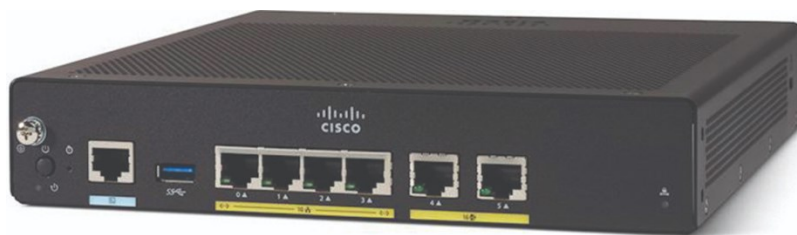


Рисунок 2.4 – Вигляд роутера моделі Cisco C921-4P LAN маршрутизатор WAN 2x GE, LAN 4x GE

2 x GE LAN порти Ethernet 4 x GE

Пам'ять FLASH 2 Гб

Об'єм ОЗУ 1 Гб

Тип живлення AC 100-240В

Висота RM UNIT 1U

Тип установки Настільне

Порти консольні RJ-45

Порти USB 1 x USB 2.0

2 x GE LAN порты Ethernet 4 x GE

Память FLASH 2 Гб

Объем ОЗУ 1 Гб

Тип питания AC 100-240В

Высота RM UNIT 1U

Тип установки Настольное

Порты консольные RJ-45

Порты USB 1 x USB 2.0



Рисунок 2.5 – Вигляд точкою доступу моделі Cisco AIR-AP3802I-R-K9

Cisco UCS сервери призначені для роботи критично важливих програм та сервісів, що потребують інтенсивної обробки даних, обчислень та використовують великі обсяги пам'яті. Ці пристрої корпоративного класу використовують переважно у великих організаціях, які приймають прості мережного устаткування.

Серії Cisco UCS серверів



Cisco UCS сервери засновані на перспективній платформі Cisco UCS з її орієнтацією на роботу у навантаженій волоконно-оптичній інфраструктурі, відкритими інтерфейсами API, а також із глибоким апаратним віртуалізацією. Архітектурна перевага Cisco UCS полягає в блоковій компонуванні з резервуванням, використанням новітніх процесорів, великих обсягів ОЗП і масивів жорстких дисків HDD або SSD.

Ці сервери представлені трьома серіями:

Cisco UCS E-Series (блейд-сервери)

Cisco UCS B-Series (блейд-сервери)

Cisco UCS C-Series (Стійкові сервери)

Переваги використання

Cisco Unified Computing System – це уніфіковане рішення, яке дозволяє мінімізувати загальну кількість мережного обладнання для обслуговування мереж. До основних рішень, які застосовуються у цих пристроях, можна віднести такі:

Cisco Unified Computing System. Уніфікація мережного обладнання, інструментів обчислення, а також схем доступу до систем зберігання даних забезпечує універсальний та простий підхід до розгортання та масштабування мереж у великих корпораціях.

Спільнота партнерів Cisco із впровадження технологій уніфікованих обчислень. Використовуючи рішення на базі Cisco Unified Computing System, можна розгорнути мережі з індивідуальними стандартами для різних сфер діяльності.

Сумісність із системами зберігання даних. Cisco Unified Computing System підтримує продукти Emulex, Qlogic, EMC, NetApp та інші, призначені для використання в системах зберігання даних.

Сумісність із програмним забезпеченням. Cisco Unified Computing System має всі відповідні сертифікати, які забезпечують сумісність із найчастіше використовуваними програмами корпоративного рівня, системами віртуалізації та операційними системами.

Прискорене розгортання. Звичні терміни розгортання протягом кількох діб скорочуються до кількох годин завдяки простому алгоритму налаштувань.

Можливість оцінки архітектурної системи. Спеціальні інструменти з метою оцінки ефективності мережевої архітектури дозволяють визначити відповідність конфігурації серверного устаткування заданим параметрам мережі.

Планування та проектування мереж. До цих послуг можна віднести підвищення продуктивності з розширенням мережі, можливості впровадження нових технологій, а також зниження потреб в оновленні обладнання у разі підвищення вимог до мережі.

Уніфіковані обчислення. Ви можете активно використовувати хмарні послуги за допомогою новітніх технологій віртуалізації. Крім того, інтеграція з програмами на базі Oracle, Microsoft і UNIX забезпечує захист інвестицій та значне підвищення продуктивності.

#### Технічні специфікації

Висока продуктивність та ефективність роботи досягаються завдяки низці технічних та програмних особливостей Cisco UCS серверів.

Потужні процесори. Інноваційні багатоядерні процесори сімейства Intel Xeon® за допомогою технологій Intel Turbo Boost та Intel Intelligent Power автоматично адаптують витрату енергії та рівень продуктивності згідно навантажень від мережевих програм.

Відкритий інтерфейс. Open XML API надає до 9000 точок інтеграції та забезпечує взаємодію із вже існуючими інструментами управління.

Одноразове підключення. Технологія Cisco Single Connect забезпечує значне спрощення волоконних підключень мереж та кабельної інфраструктури: один простий та ефективний спосіб підключення стійки та блейд-серверів у фізичних та віртуальних середовищах LAN та SAN для керування ними.

Волоконне підключення. Ця особливість забезпечує функції розширення, підвищення продуктивності та простоти управління як у випадку з блейд-серверами, так і зі стійковими моделями. Технологія Cisco Data Center VM-FEX об'єднує віртуальну та фізичну мережу в єдину інфраструктуру. Адміністратори центрів обробки даних тепер можуть встановлювати налаштування, конфігурувати, керувати, контролювати та діагностувати мережевий трафік як віртуальних машин, так і в середовищах із виключно апаратним обладнанням у рамках єдиної інфраструктури.



Рисунок 2.6 – Вигляд Cisco сервер C240M4-Standard-1

Серія Cisco UCS C-Series

Процесор Intel Xeon E5-2630 v3 2.4 ГГц

Слоти HDD 12 x 3.5" SATA III

Слоти інтерфейсних карт 1 слот

Об'єм ОЗУ 128 Гб

Пам'ять ОЗУ максимум 768 Гб

Висота RM UNIT 2U

Відео виходи VGA (D-Sub 15)

Порти USB 2 x USB 3.0

Інтерфейс Ethernet 2 x GE RJ-45

Застосування панорамних IP-відеокамер є максимально ефективним для побудови зовнішнього відеомоніторингу. Пристрої можна використовувати для спостереження за людськими потоками, за територіями підприємства, прибудинковими майданчиками, паркінгами та автостоянками, зупинками та транспортними розв'язками, вокзалами та аеропортами.

## Панорамні камери Axis

Сьогоднішній ринок систем мережевого відеоспостереження розвивається за рахунок закордонних виробників, лідером серед яких є компанія Axis Communications. Продукція бренду представлена у нашому асортименті.

Панорамні камери Axis, як правило, є фіксованими пристроями куполоподібної форми, оснащеними ширококутним об'єктивом типу «риб'яче око». Вони мають компактні габарити та міцний корпус, можуть монтуватись як на стелю (круговий огляд на 360 градусів), так і на стіну (панорама на 180 градусів). У комплект поставки в більшості випадків входять спеціальні кріпильні деталі для підвісного, накладного та врізного монтажу.

Вуличні панорамні камери Axis мають антивандальну конструкцію – вони стійкі до будь-яких механічних ударів, спроб розкрити корпус, нанести пошкодження або зафарбувати об'єктив фарбою. У таких форс-мажорних ситуаціях камера передає сигнал тривоги.

### Особливості панорамних камер Axis

Безшовний перегляд, що дозволяє імітувати перегляд одночасно з чотирьох відеокамер; пересування об'єктів на ділянці відстежується без втрати їх з виду у проміжках між камерами;

Розширення 5 Мпкс при швидкості 30 кадрів на секунду забезпечує високу якість зйомки за таких великих параметрів;

Надійність та максимальний рівень безпеки. Прогресивні цифрові алгоритми роботи захищають пристрої від збоїв, вірусних атак та несанкціонованого вторгнення;

Підтримка технології PoE (Power over Ethernet), яка дозволяє жити камеру через мережу Ethernet; немає потреби прокладати додаткові кабелі.

Підтримка аудіо, можливість підключити різні аудіопристрої, отримувати окрім зображення аудіоінформацію, а також надсилати на пристрій голосові вказівки.

Робота на основі власного програмного забезпечення AXIS Camera Station, що спрощує керування відеоспостереженням.

Сумісність з інтелектуальними програмами (наприклад, підрахунок людей на записи або відображення температурних градієнтів) за допомогою платформи прикладних програм AXIS.

Переваги IP-камера від Axis

Бездоганна якість зображення з високою роздільною здатністю;

Легкість у встановленні та застосуванні;

Віддалений та бездротовий доступ до відеоінформації;

відсутність необхідності віддаленого сервера або центрального комп'ютера;

Масштабованість;

Пристосованість до сучасних реалій: можливість переглядати відео на iPhone, iPad та пристрої на платформі Android.

Модельний ряд

Модельний ряд панорамних IP камер від виробника Axis не дуже широкий через специфіку та унікальність даного обладнання. Моделі, представлені на ринку, відрізнятимуться роздільною здатністю відео, кутом огляду, наявністю слота картки пам'яті MicroSD/MicroSDHC, підтримкою режиму день/ніч.

У плані функціональності та доступності цікавою є модель M3007-PV. Це фіксована 5-мегапксельна камера купольного типу, яка оптимально підходить для відеоспостереження невеликих магазинів, готелів, місць громадського харчування. Пристрій забезпечить чіткий та якісний панорамний огляд на 180 ° або 360 °. Площа охопленої території M3007-PV може досягати 650 м<sup>2</sup>. До переваг цієї моделі можна віднести міцний корпус, захищений від актів вандалізму, стійкість до пилу, прямим сонячним променям, температурним перепадам. Усередині приміщення пристрій легко виявить підозрілу активність, а зовні - чудово впорається з відстеженням

поток людей, що дозволить ефективно контролювати довірену територію об'єкта.

З відеоспостереженням великих об'єктів (площ та вулиць, торгових центрів та паркінгів, вокзалів та аеропортів) краще за інших впоратися флагманська панорамна камера купольного типу Q6045-E від Axis. Дана модель може похвалитися унікальною роздільною здатністю - HDTV 1080p. Для чіткості та приголомшливої деталізації зображення використовується 32-кратний оптичний зум. До переваг пристрою також можна віднести легкість, швидкість і точність управління панорамуванням та нахилом, захист найвищого класу від вандалізму, стійкість до стрибків напруги, температурних перепадів, погодних сюрпризів (снігопади, спека, злива). Ця модель розрахована на денну та нічну зйомку. Живлення пристрою здійснюється за технологією High PoE.



Рисунок 2.7 - M3027-PVE AXIS панорамная IP-камера купольная PoE 5MP (2592x1944), 187°, 1/3.2", f=1.27mm, F2.0, SD

Серія AXIS M30

Горизонтальний кут огляду 187°

Роздільна здатність відео Max: 2592 x 1944

Потужність номінальна/максимальна 4,5 Вт

Тип живлення PoE  
Тип установки Настінне/стельове  
Підтримувані відеокодеки H.264  
Блок живлення у комплекті Ні  
Карта пам'яті SD Так  
Фокусна відстань  $f=1.3\text{mm}$   
Температура експлуатації від  $-30\text{ }^{\circ}\text{C}$  до  $50\text{ }^{\circ}\text{C}$   
Діафрагма F2.0  
Детектування руху Є  
Сенсор 1/3.2" CMOS 5M  
Мінімальна освітленість 0.6lux  
Інтерфейс Ethernet 1 x FE RJ-45

Структурована кабельна система є кабельною проводкою, що реалізується відповідно до певних стандартів. Основною відмінністю СКС від ЛОМ є її незалежність від додатків, які будуть використовуватись згодом, що дозволяє їй підтримувати широкий діапазон додатків. Відповідність СКС стандартам дає можливість інтегрувати до єдиної інформаційної структури:

- комп'ютерну (ЛВС) та телефонну мережу (МС);
- засоби охоронної та пожежної сигналізації (ОПС);
- охоронне відеоспостереження (СОВН) та ІР-відеоспостереження;
- систему контролю управління доступом (СКУД) та звукового оповіщення;
- телебачення та радіо тощо.

Структурована кабельна система - універсальна кабельна система будівлі (або комплексу будівель), побудована за правилами, що визначаються міжнародними стандартами:

ISO/IEC 11801: 2002(E), Information Technology Generic Cabling for Customer Premises (інформаційна технологія загального каблювання приміщень замовника).

ANSI/TIA/EIA-568-B, Commercial Building Telecommunications Cabling Standard (стандарт телекомунікаційних кабельних систем комерційних будівель).

СКС може бути побудована на основі безлічі продуктів різних виробників із застосуванням двох основних середовищ передачі сигналу - мідна кручена пара і волоконна оптика.

Структурована кабельна система СКС може бути реалізована як серед групи будівель, так і в окремій будівлі. Вона може складатися із трьох підсистем, які можуть з'єднуватися в мережу, що має топологію "зірка".

#### Топологія

СКС є кабельною проводкою, що реалізується відповідно до певних стандартів. Основною відмінністю СКС від ЛОМ є її незалежність від додатків, які будуть використовуватись згодом, що дозволяє їй підтримувати широкий діапазон додатків.

Відповідність СКС стандартам дає можливість інтегрувати в єдину інформаційну структуру комп'ютерну мережу, ЛОМ, телефонну мережу, засоби охоронної та пожежної сигналізації, охоронне відеоспостереження та ІР-відеоспостереження; систему контролю управління доступом та звукового оповіщення; телебачення та радіо тощо.

Термін служби подібної інфраструктури незмірно більший, ніж у окремих пристроїв мережі, і чим вище існує розуміння необхідності інвестицій у структуровані кабельні системи та системи безпеки підприємства, тим вище на Вас чекає економія в перспективі. Побудова самої комп'ютерної мережі може мати кілька різних топологій: зірка, загальна шина, дерево або бути закольцованною і наприклад у межах однієї будівлі відрізняється горизонтальну складову і магістральну.

Горизонтальна кабельна система – поверхова система будівлі, що з'єднує телекомунікаційні розетки на робочому місці (Work Area – WA) з горизонтальним кросом (Floor Distribution – FD), розташованим у



телекомунікаційній. FD може розташовуватися на тому ж або на суміжному поверсі.

Магістральна кабельна система всередині будівлі - кабельна система (СКС), що з'єднує кожен горизонтальний крос (FD) всередині однієї будівлі з головною (Campus Distribution - CD) або кросом будівлі (Building Distribution - BD).

Магістральна кабельна система між будинками - кабельна система, що зв'язує будівлі серед групи будівель. Кожен кабель зовнішньої магістралі проходить від головного кросу (CD) (розташованого зазвичай у центральному будинку) до проміжного кросу (BD).

#### **2.2.4 Захист інформації в комп'ютерній системі**

На торгівельному мережевому підприємстві інформація розділяється на загальнодоступну та конфіденційну. Враховуючи особливості мережевої організації комп'ютерної системи підприємства необхідно забезпечити інформаційну безпеку.

##### **2.2.4.1 Особливості інформаційної безпеки мережевих операційних систем**

Адміністратор безпеки повинен налаштувати операційну систему, в середовищі якої планується використовувати СКЗІ, та здійснювати періодичний контроль зроблених налаштувань відповідно до таких вимог:

Правом установки та налаштування ОС та СКЗІ повинен мати лише адміністратор безпеки.

Всім користувачам та групам, зареєстрованим в ОС, необхідно призначити мінімально можливі для нормальної роботи права.

У групи Everyone мають бути видалені всі привілеї.

Рекомендується виключити використання автоматичного входу користувача в операційну систему під час її завантаження.

Рекомендується перейменувати стандартний обліковий запис Administrator.

Потрібно відключити обліковий запис для гостьового входу Guest.

Виключити можливість віддаленого керування, адміністрування та модифікації ОС та її налаштувань, системного реєстру для всіх, включаючи групу Administrators.

Усі ресурси системи, що не використовуються, необхідно відключити (протоколи, послуги тощо).

Повинне бути виключено або обмежено з урахуванням обраної в організації політики безпеки використання користувачами Scheduler (планувальник завдань). При використанні даного сервісу склад програмного забезпечення, що запускається, на АРМ узгоджується з адміністратором безпеки.

Рекомендується організувати затирання тимчасових файлів та файлів підкачування, що формуються або модифікуються в процесі роботи СКЗІ. Якщо це нездійснено, то ОС повинна використовуватися в режимі одного користувача і на жорсткий диск повинні поширюватися вимоги, що пред'являються до ключових носіїв.

Повинні бути встановлені обмеження на доступ користувачів до системного реєстру відповідно до прийнятої в організації політики безпеки, що реалізується за допомогою ACL або встановлення прав доступу за наявності NTFS.

На всі директорії, що містять системні файли Windows та програми з комплекту СКЗІ, повинні бути встановлені права доступу, що забороняють запис усім користувачам, крім Адміністратора (Administrator), Творця/Власника (Creator/Owner) та Системи (System).

Має бути виключена можливість створення аварійного дампа оперативної пам'яті, оскільки він може містити криптографічно небезпечну інформацію.

Рекомендується забезпечити ведення журналів аудиту в ОС, у своїй вона має бути налаштована завершення роботи під час переповнення журналів.

Рекомендується налаштувати параметри системного реєстру відповідно до експлуатаційної документації на СКЗІ.

Рекомендується розробити та застосувати політику призначення та зміни паролів (для входу в ОС, BIOS, при шифруванні на паролі тощо), використовувати фільтри паролів відповідно до таких правил:

довжина пароля має бути не менше 6 символів;

у числі символів пароля обов'язково повинні бути літери у верхньому та нижньому регістрах, цифри та спеціальні символи (@, #, \$, &, \*, % тощо);

пароль не повинен включати легко обчислювані поєднання символів (імена, прізвища і т.д.), а також загальноприйняті скорочення (USER, ADMIN, ALEX і т.д.);

при зміні пароля нове значення повинне відрізнятися від попереднього не менш як у 4-х позиціях;

особистий пароль користувач не має права повідомляти нікому;

не допускається зберігати записані паролі у легкодоступних місцях;

періодичність зміни пароля визначається прийнятою політикою безпеки, але має перевищувати 6 місяців;

зазначена політика є обов'язковою для всіх облікових записів, зареєстрованих в ОС.

#### **2.2.4.2 Особливості взаємодії інформаційної системи з мережами загального користування**

При використанні СКЗІ на АРМ, підключених до мереж загального користування, повинні бути вжиті додаткові заходи, що виключають можливість несанкціонованого доступу до системних ресурсів операційних систем, що використовуються, до програмного забезпечення, в оточенні якого функціонують СКЗІ, і до компонентів СКЗІ з боку зазначених мереж.

Як такий захід рекомендується встановлення та використання на АРМ засобів міжмережевого екранування. Повинний бути закритий доступ до всіх портів, що не використовуються. У разі підключення АРМ із встановленим СКЗІ до загальнодоступних мереж передачі даних необхідно обмежити можливість відкриття та виконання файлів та скриптових об'єктів (JavaScript, VBScript, ActiveX тощо), отриманих із мереж загального користування, без проведення відповідних перевірок щодо змісту в них програмних даних, закладок та шкідливих програм.

В організації має бути визначено та затверджено порядок обліку, зберігання та використання носіїв ключової інформації з ключами ЕП та шифрування, який повинен виключати можливість несанкціонованого доступу до них.

Для зберігання ключових носіїв у приміщеннях повинні встановлюватись надійні металеві сховища (сейфи), обладнані надійними замикаючими пристроями.

Забороняється:

Знімати несанкціоновані адміністратором безпеки копії з ключових носіїв.

Знайомити із вмістом ключових носіїв або передавати ключові носії особам, які до них не допущені, а також виводити ключову інформацію на дисплей (монітор) АРМ або принтер.

Встановлювати ключовий носій в пристрій, що зчитує ПЕОМ АРМ в режимах, не передбачених функціонуванням системи, а також встановлювати носій в інші ПЕОМ.

Записуйте на ключовий носій сторонню інформацію.

Власник сертифіката ключа перевірки ЕП зобов'язаний:

Зберігати у таємниці ключ ЕП (закритий ключ).

Не використовувати для електронного підпису та шифрування ключі, якщо відомо, що ці ключі використовуються або використовувалися раніше.

Негайно вимагати зупинення дії сертифіката ключа перевірки ЕП за наявності підстав вважати, що таємниця ключа ЕП (закритого ключа) порушена (відбулася компрометація ключа).

Оновлювати сертифікат ключа перевірки ЕП відповідно до встановленого регламенту.

Дії, пов'язані з експлуатацією СКЗІ, повинні фіксуватися в «Журналі користувача мережі», який веде особа, яка відповідає за забезпечення інформаційної безпеки на АРМ. У журнал крім цього записуються факти компрометації ключових документів, позаштатні ситуації, що відбуваються в системі та пов'язані з використанням СКЗІ, проведення регламентних робіт, дані про отримані у адміністратора безпеки організації ключові носії, позаштатні ситуації, що відбулися на АРМ, із встановленим ПО СКЗІ. У журналі може відображатися така інформація:

дата час;

запис про компрометацію ключа;

запис про виготовлення особистого ключового носія користувача;  
ідентифікатор носія;

запис про виготовлення копій особистого ключового носія користувача; ідентифікатор носія;

запис про виготовлення резервного ключового носія користувача;  
ідентифікатор носія;

запис про отримання сертифіката ключа перевірки ЕП, повний номер ключового носія, який відповідає сертифікату;

записи, що відображають видачу на руки користувачам (відповідальним виконавцям) та здачу ними на зберігання особистих ключових носіїв, включаючи резервні ключові носії;

події, що відбувалися на АРМ користувача із встановленим ПО СКЗІ, із зазначенням причин та вжитих дій.

Користувач (або адміністратор безпеки) повинен періодично (не рідше одного разу на два місяці) проводити контроль цілісності та легальності

встановлених копій ПЗ на всіх АРМ із вбудованою СКЗІ за допомогою програм контролю цілісності, переглядати повідомлення про події в журналі EventViewer операційної системи, а також проводити періодичне тестування технічних та програмних засобів захисту.

У разі виявлення «сторонніх» (не зареєстрованих) програм, порушення цілісності програмного забезпечення або виявлення факту пошкодження печаток на системних блоках робота на АРМ має бути припинена. За цим фактом має бути проведене службове розслідування комісією, призначеною керівником організації, де сталося порушення, та організовано роботи з аналізу та ліквідації негативних наслідків цього порушення.

Рекомендується організувати на АРМ систему аудиту відповідно до політики безпеки, прийнятої організації, з регулярним аналізом результатів аудиту.

#### **2.2.4.3 Особливості програмного забезпечення автоматизованих робочих місць системи**

На технічних засобах АРМ із встановленим СКЗД необхідно використовувати лише ліцензійне програмне забезпечення фірм-виробників, отримане з довірених джерел.

На АРМ має бути встановлена лише одна операційна система. При цьому не допускається використовувати нестандартні, змінені або налагоджувальні версії операційної системи.

Не допускається встановлення на АРМ засобів розробки та налагодження програмного забезпечення. Якщо засоби налагодження програм необхідні для технологічних потреб користувача, їх використання має бути санкціоновано адміністратором безпеки. У будь-якому випадку забороняється використовувати ці засоби для перегляду та редагування коду та пам'яті програм, що використовують СКЗІ. Необхідно виключити попадання в систему коштів, що дозволяють здійснювати несанкціонований

доступ до системних ресурсів, а також програм, що дозволяють, користуючись помилками ОС, отримувати привілеї адміністратора.

Рекомендується обмежити можливості користувача запуском лише тих програм, які дозволені адміністратором безпеки.

Рекомендується встановити та використовувати антивірусне програмне забезпечення на АРМ.

Необхідно регулярно відстежувати та встановлювати оновлення безпеки для програмного забезпечення АРМ (Service Packs, Hot fix тощо), оновлювати антивірусні бази.

Рекомендується використовувати АРМ з СКЗІ в режимі одного користувача. В окремих випадках, при необхідності використання АРМ кількома особами, ці особи повинні мати рівні права доступу до інформації.

Не дозволяється залишати без контролю АРМ при включеному живленні та завантаженому програмному забезпеченні СКЗД після введення ключової інформації. При виході користувача з робочого місця повинно використовуватися автоматичне увімкнення заставки, захищеної паролем. В окремих випадках за неможливості використання парольного захисту допускається завантаження ОС без запиту пароля, при цьому повинні бути реалізовані додаткові організаційно-режимні заходи, що унеможливають несанкціонований доступ до АРМ.

Рекомендується передбачити заходи, що унеможливають несанкціоновану зміну апаратної частини АРМ, наприклад, опечатування системного блоку АРМ адміністратором. Також можливе з цією метою застосування спеціальних засобів захисту інформації - апаратних модулів довіреного завантаження.

### 3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

#### 3.1 Розрахунок адресації комп'ютерної мережі та схеми адресації пристроїв

Одним із найважливіших завдань кваліфікаційної роботи є проектування корпоративної комп'ютерної мережі підприємства.

Після розробки адресації необхідно використати PacketTracer для розробки імітаційної моделі і перевірки працездатності спроектованої мережі.

Адреса для виділення підмереж: 172.23.224.0/21.

Кількість вузлів приведена в таблиці 4.1. Налаштування паролів базової конфігурації пристроїв приведені у таблиці 3.2.

Таблиця 3.1 – Кількість вузлів у підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
45	12	25	6	8

LAN1 – локальна мережа, яка об'єднує підрозділи з підключенням 45 терміналів.

LAN2 – локальна мережа, яка об'єднує 12.

LAN3 – об'єднує 25 терміналів центрального офісу та складу.

LAN4 – локальна мережа яка об'єднує 6.

LAN5 – локальна мережа, яка об'єднує 8.

Таблиця 3.2 – Налаштування паролів базової конфігурації пристроїв

Паролі		
консолі і vty	привілейованого режиму	користувача
<i>cisco12320sk</i>	<i>class12320sk</i>	<i>Cherkasskiy</i>



Технологія VLSM (Variable Length Subnet Masks, RFC 950) дозволяє використання більш ніж однієї маски в мережах одного адресного простору. Застосування таких масок змінної довжини забезпечує заощадливіше використання адресного простору.

Виділений блок 172.23.224.0/21 дає можливість адресувати 2046 пристроїв.

Для мережі LAN1 на 45 вузлів:

маска 255.255.255.192 (або префікс /26). Діапазон адрес 172.23.224.1 - 172.23.224.62. Широкомовлення 172.23.224.63. Для адресації 45 пристроїв використовуємо адреси 172.23.224.3 - 172.23.224.48.

Мережа LAN2 на 12 вузлів, маска 255.255.255.240 (або префікс /28). Діапазон адрес 172.23.224.97 - 172.23.224.110. Широкомовлення 172.23.224.111. Для адресації 12 пристроїв використовуємо адреси 172.23.224.97 - 172.23.224.110.

Для мережі LAN3 на 25 вузлів:

маска 255.255.255.224 (або префікс /27). Діапазон адрес 172.23.224.65 - 172.23.224.94. Широкомовлення 172.23.224.95. Для адресації 25 пристроїв використовуємо адреси 172.23.224.67 - 172.23.224.92.

Для мережі LAN4 на 6 вузлів:

маска 255.255.255.248 (або префікс /29). Діапазон адрес 172.23.224.129 - 172.23.224.134. Широкомовлення 172.23.224.135. Для адресації 6 пристроїв використовуємо адреси 172.23.224.129 - 172.23.224.134.

Для мережі LAN5 на 8 вузлів:

маска 255.255.255.240 (або префікс /28). Діапазон адрес 172.23.224.113 - 172.23.224.126. Широкомовлення 172.23.224.127. Для адресації пристроїв використовуємо адреси 172.23.224.114 - 172.23.224.122.

Аналогічно адресуємо з'єднання між маршрутизаторами WAN (табл.3.3).

Таблиця 3.3 – Схема адресування мережі

Ім'я мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
LAN1	45	172.23.224.0	255.255.255.192	172.23.224.3	172.23.224.48
LAN2	12	172.23.224.96	255.255.255.240	172.23.224.97	172.23.224.110
LAN3	25	172.23.224.64	255.255.255.224	172.23.224.67	172.23.224.92
LAN4	6	172.23.224.128	255.255.255.240	172.23.224.129	172.23.224.134
LAN5	8	172.23.224.112	255.255.255.248	172.23.224.114	172.23.224.122
WAN1	2	10.0.2.0	255.255.255.252	10.0.2.1	10.0.2.2
WAN2	2	10.0.2.4	255.255.255.252	10.0.2.5	10.0.2.6
WAN3	2	10.0.2.8	255.255.255.252	10.0.2.9	10.0.2.10
WAN4	2	10.0.2.12	255.255.255.252	10.0.2.13	10.0.2.14
WAN5	2	10.0.2.16	255.255.255.252	10.0.2.17	10.0.2.18
WAN6	2	10.0.2.20	255.255.255.252	10.0.2.21	10.0.2.22
WAN7	2	10.0.2.24	255.255.255.252	10.0.2.25	10.0.2.26
WAN8	2	10.0.2.28	255.255.255.252	10.0.2.29	10.0.2.30

В таблиці 3.4 наведені адреси всіх пристроїв у мережі.

Таблиця 3.4 – Адреси всіх пристроїв у мережі

Ім'я пристрою	Інтерфейс	IP адреса	Маска	Шлюз	VLAN	Для ПК інтерфейс підключеного пристрою
(LAN 1)						
Cherkasskiy _ Rout3	G0\0	172.23.224.1	/26			Sw1_Fa0
	G0\1	10.0.2.1	/30			IPS_G0/1
	G0\2	10.0.2.5	/30			R4_G0/0
	G0\3	10.0.2.9	/30			R1_G0/1
Cherkasskiy _ Sw1	Vlan1	172.23.224.2	/26	172.23.224.1		R3_G0/0
PC1_1-PC1_45	NIC	172.23.224.3- 172.23.224.48	/26	172.23.224.1		-
Server HTTP	Fa0	172.23.224.49	/26	172.23.224.1		-
Server DNS	Fa0	172.23.224.50	/26	172.23.224.1		-
(LAN 2)						
Cherkasskiy _ Rout5	G0\0	172.23.224.97	/28			Sw2_Fa0
	G0\1	10.0.2.13	/30			R1_G0/2

	G0\2	10.0.2.17	/30			R2_G0/1
Cherkasskiy _ Sw2	Vlan1	172.23.224.98	/28	172.23.224.97		R5_G0/0
PC2_1 – PC2_108	NIC	172.23.224.99 - 172.23.224.110	/28	172.23.224.97		-
(LAN 3)						
Cherkasskiy _ Rout0	G0\0	172.23.224.65	/27			Sw3_Fa0
	G0\1	10.0.2.21	/30			ISP_G0/0
Cherkasskiy _ Sw3	Vlan1	172.23.224.66	/27	172.23.224.65		R0_G0/0
PC3_1 – PC3_25	NIC	172.22.49.3 - 172.22.49.111	/27	172.23.224.65		
(LAN 4)						
Cherkasskiy _ Rout1	G0\0	172.23.224.129	/29			Sw4_Fa0
	G0\1	10.0.2.10	/30			R3_G0/3
	G0\2	10.0.2.14	/30			R5_G0/1
Cherkasskiy _ Sw4	Vlan1	172.23.224.130	/29	172.23.224.129		R1_G0/0
PC4_1 – PC4_4	NIC	172.23.224.131 -172.23.224.134	/29	172.23.224.129		-
(LAN 5)						
Cherkasskiy _ Rout2	G0\0	172.23.224.113	/28			Sw5_Fa0
	G0\1	10.0.2.18	/30			R5_G0/2
	G0\2	10.0.2.25	/30			R4_G0/1
Cherkasskiy _ Sw5	Vlan1	172.23.224.114	/28	172.23.224.113		R2_G0/0
PC5_1-PC5_8	NIC	172.23.224.116 - 172.23.224.122	/28	172.23.224.113		-
Server TFTP	Fa0	172.23.224.115	/28	172.23.224.113		-
(LAN 6)						
Cherkasskiy _ Rout4	G0\0	10.0.2.6	/30			R3_G0/2
	G0\1	10.0.2.26	/30			R2_G0/2
ISP	G0\0	10.0.2.22	/30			R0_G0/1
	G0\1	10.0.2.2	/30			R3_G0/1
	G0\2	209.165.201.5	/30			PC00
PC00	Fa0	209.165.201.6	/30	209.165.201.5		ISP_G0/2

Віртуальні локальні мережі були створені для вирішення питання розподілу повноважень та впровадження політик безпеки без використання дорогих рішень та приладів. VLAN дозволяє розділяти користувачів не за їх територіальною приналежністю, а за логічним розподілом функцій та призначення. Наприклад, в одній кімнаті можуть знаходитись люди, що є менеджерами з різних напрямків.

Таблиця 3.5 - Адресація мережі

Ім'я мережі	Кількість вузлів	Адреса мережі	Маска під мережі	Початкове значення	Кінцеве значення
VLAN10	10	10.42.9.64	255.255.255.224	10.42.9.65	10.42.9.75
VLAN20	10	10.42.9.32	255.255.255.224	10.42.9.33	10.42.9.43
VLAN30	10	10.42.9.0	255.255.255.224	10.42.9.1	10.42.9.11
VLAN99	10	10.42.9.160	255.255.255.0	10.42.9.161	10.42.9.171

#### Налаштування VLAN на комутаторі LAN1

```
Lan1(config)#int g0/1
```

```
Lan1(config-if)# switchport mode trunk
```

```
Lan1(config-if)# switchport trunk native vlan 100
```

```
Lan1(config-if)# switchport trunk allowed vlan 10,20,30,99
```

```
Lan1(config-if)#int range f0/1-2
```

```
Lan1(config-if-range)# switchport mode trunk
```

```
Lan1(config-if-range)# switchport trunk native vlan 100
```

```
Lan1(config-if-range)# switchport trunk allowed vlan 10,20,30,99
```

```
Lan1(config-if-range)# int range f0/0-5
```

```
Lan1(config-if-range)# switchport mode access
```

```
Lan1(config-if-range)# switchport access vlan 99
```

```
Lan1(config-if-range)# int range f0/6-10
```

```
Lan1(config-if-range)# switchport mode access
```

```
Lan1(config-if-range)# switchport access vlan 30
```

```
Lan1(config-if-range)# int range f0/10-15
```

```
Lan1(config-if-range)# switchport mode access
```

```

Lan1(config-if-range)# switchport access vlan 20
Central (config)# int g0/1.30
Central (config-if)# encapsulation dot1Q 20
Central (config-if)# ip address 10.42.9.54 255.255.255.224
Central (config-if)# int g0/1.20
Central (config-if)# encapsulation dot1Q 20
Central (config-if)# ip address 10.42.9.37 255.255.255.224
Central (config-if)# int g0/1.30
Central (config-if)# encapsulation dot1Q 30
Central (config-if)# ip address 10.42.9.1 255.255.255.224

```

### 3.2 Розробка моделі та перевірка роботи комп'ютерної системи

Доцільно провести перевірку розрахунку адресації на розроблений для цього моделі. Використання Cisco Packet Tracer дозволяє це зробити. А також можемо провести перевірку базових налаштувань мережевого обладнання.

Моделі розробленої мережі показана на рисунку 3.1.

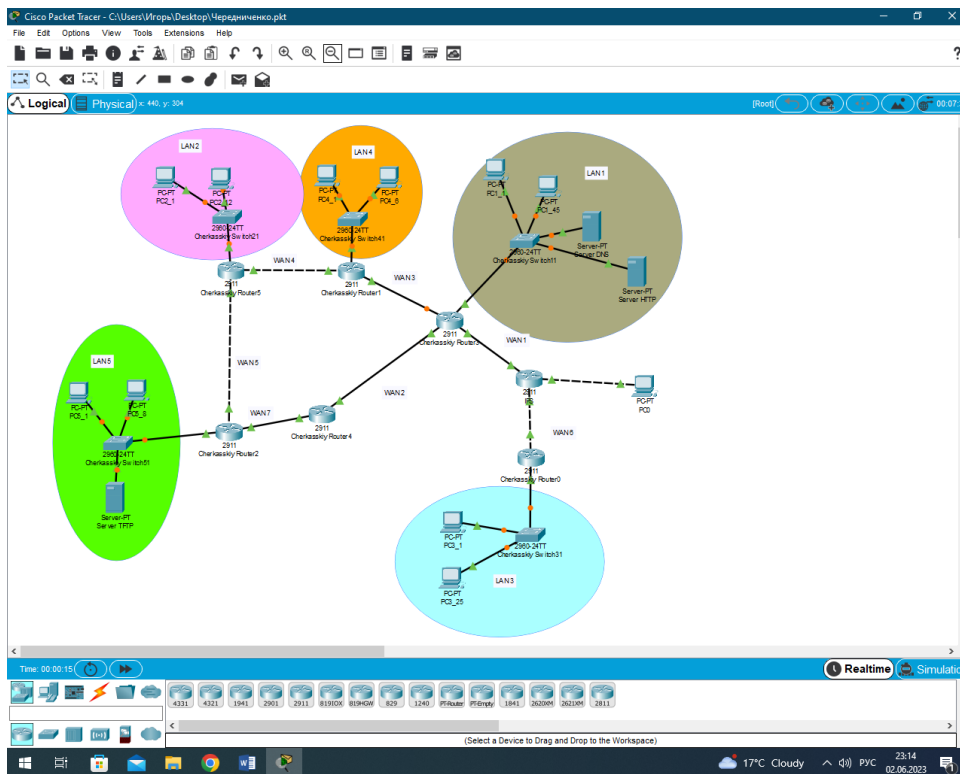


Рисунок 3.1 – Схема моделі мережі



Налаштування виконувалося як за допомогою графічного інтерфейсу, так і за допомогою IOS command line interface.

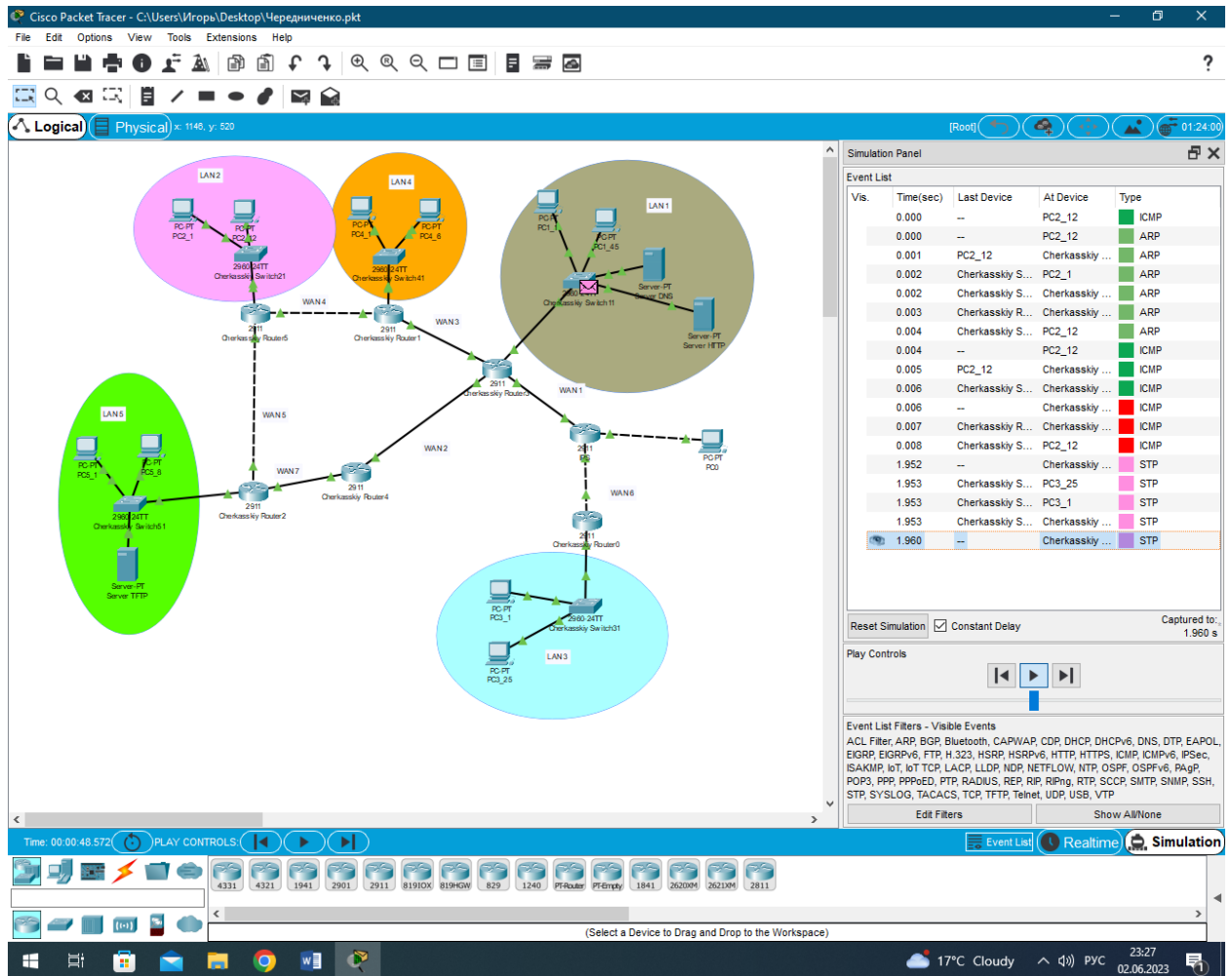


Рисунок 3.3 – Перевірка проходження пакетів між елементами моделі

В результаті симуляції роботи мережі показано, що пакети з інформацією успішно проходять через мережу по своїй адресі.

### 3.2.1 Базове налаштування конфігурації пристроїв

Маршрутизатор серії Cisco 2900 забезпечують високу продуктивність, безпеку і інтеграцію багатьох сервісів, є рішення для компаній, діяльність яких залежить від технологій. Багатий набір інтегрованих послуг, функції підтримки мультимедіа і неперевершена ефективність роботи може повністю

змінити місце роботи. Маршрутизатор серії Cisco 2900 забезпечують високу продуктивність, безпеку і інтеграцію багатьох сервісів, є рішення для компаній, діяльність яких залежить від технологій. Багатий набір інтегрованих послуг, функції підтримки мультимедіа і неперевершена ефективність роботи може повністю змінити місце роботи. Безпечний доступ до зовнішньої мережі за допомогою підключення 3G забезпечує безперервність бізнесу, підтримка продукту Cisco Unified Communications Manager Express забезпечує безпечну спільну роботу для до 150 користувачів. Підтримка VPN забезпечує безпечний обмін даними і спільну роботу з допомогою технологій:

GETVPN (Group Encrypted Transport VPN),

DMVPN (Dynamic Multipoint VPN),

Enhanced Easy VPN.

Комутатори Cisco - це стекові автономні комутатори з фіксованою конфігурацією, які призначені для інфраструктури мереж Fast Ethernet і Gigabit Ethernet і забезпечують продуктивність на швидкості середовища передачі. Комутатори поставляються з двома типами програмного забезпечення і в самих різних конфігураціях, завдяки чому можна підібрати підходящий варіант для будь-якого підприємства малого і середнього бізнесу, а також віддалених філій і виробничих середовищ. Програмне забезпечення Standard Image пропонує базові функції програмного забезпечення Cisco IOS для передачі даних, голосу і відео. Для інтелектуальних мереж, яким потрібні додаткові функції безпеки, розширені можливості управління якістю обслуговування і високий рівень доступності на кордоні мережі, призначене програмне забезпечення Enhanced Image (EI), що включає підтримку таких функцій, як обмеження швидкості і фільтрація трафіку.

Для безпечного доступу до пристроїв необхідно задати на всіх пристроях до консолі і vty cisco, а також задати пароль до привілейованого режиму class та зашифрувати всі паролі, що зберігаються у відкритому виді.



Також налаштуємо банер, що буде відображатись при підключенні маршрутизатора.

```

Cherkasskiy_Router1(config)#line con 0
Cherkasskiy_Router1(config)#password cisco
Cherkasskiy_Router1(config)#login
Cherkasskiy_Router1(config)#lyne vty 0 4
Cherkasskiy_Router1(config)#password cisco
Cherkasskiy_Router1(config)#login
Cherkasskiy_Router1(config)#enable secret class
Cherkasskiy_Router1(config)#service password-encryption
Cherkasskiy_Router1(config)#banner motd # CRouter of IT depatmen #

```

### 3.3 Налаштування роботи Інтернет

Маршрутизатор повинен вміти використовувати NAT-сервіс – механізм, який робить пряме та зворотне перетворення IP-адрес локальної мережі в одну IP-адресу, під якою в інтернет «представляються» всі комп'ютери локальної мережі. Така схема є оптимальною для мережі з комп'ютерів або для невеликих офісів компаній, в яких використовуються лише звичайні робочі станції.

Переваги цієї схеми – економія «білих» IP-адрес, незалежність від провайдера (з ним не потрібно узгоджувати використання такої схеми, ні кількість робочих станцій в ній). Кількість одночасно працюючих комп'ютерів, підключених за цією схемою, може бути дуже велике і воно залежить тільки від продуктивності маршрутизатора і «ширини» (пропускної спроможності) каналу.

При налаштуванні статичних трансляцій NAT виконуються два основні завдання:

Створення зіставлення між внутрішньою локальною (inside local) адресою та внутрішніми глобальними (inside global) адресами. Наприклад,

внутрішня локальна адреса та внутрішня глобальна адреса налаштовані як статична трансляція NAT.

Після того як зіставлення налаштовано, інтерфейси, що беруть участь у трансляції, повинні бути налаштовані як внутрішні (inside) і зовнішні (outside) щодо NAT.

Пакети, що надходять на внутрішній інтерфейс маршрутизатора з налаштованої внутрішньої локальної IPv4 адреси, транслюються і потім перенаправляються у зовнішню мережу. Пакети, що надходять на зовнішній інтерфейс, адресовані настроєної внутрішньої глобальної адреси IPv4, переводяться на внутрішню локальну адресу і потім перенаправляються всередину мережі.

Налаштування відбувається за кілька кроків:

Створити статичну трансляцію між внутрішнім локальним та зовнішнім глобальним адресами. Для цього використовуємо команду `ip nat inside source static [локальний IP глобальний IP]`. Щоб видалити трансляцію, потрібно ввести команду `no ip nat inside source static`. Якщо нам потрібно зробити трансляцію не адреси на адресу, а адреси на адресу інтерфейсу, використовується команда `ip nat inside source static [локальний _IP тип_інтерфейсу номер_інтерфейсу]`.

Визначимо внутрішній інтерфейс. Спочатку зайти в режим конфігурації інтерфейсу, використовуючи команду `interface[тип номер]` та ввести команду `ip nat inside`

Так само визначити зовнішній інтерфейс, використовуючи команду `ip nat outside`.

Для доступу в Інтернет з локальної мережі необхідно динамічно транслювати всі внутрішні адреси в певну зовнішню ір адресу. У нашому випадку, так як провайдер надає тільки одну зовнішню адресу 209.165.201.1 (визначається маскою підмережі /30 в умовах прикладу), то всі адреси локальної мережі повинні транслюватися в нього.

Вказуємо список внутрішніх адрес, які будемо транслювати в зовнішній адресу.

В результаті повинен з'явитися доступ з будь-якої робочої станції локальної мережі в Інтернет за умови, що шлюзом за замовчуванням вказано внутрішня ір адреса маршрутизатора. Перевірити можна за допомогою команди ping до адреси в Інтернет з командного рядка. Бажано, щоб адреса була в цифровому вигляді, щоб виключити потенційні проблеми з DNS іменами.

### **3.4 Розрахунок основних характеристик для вихідного трафіку мережі підприємства**

Характеристики для вихідного трафіку в сегменті мережі підприємства, коли послугами одночасно користуються 100% користувачів. Характеристики такі як: коефіцієнт зайнятості обслуговуючого маршрутизатора, завантаження каналу передачі даних маршрутизатора, середню затримку кадру, середню довжину черги, середній час перебування пакета в черзі, пропускну здатність каналу [14].

Для розрахунку приймається модель ділянки мережі як модель СМО М/М/1. Результати розрахунків порівнюються із заданими параметрами комп'ютерної системи.

Дано:

кількість вузлів в мережі: 45

середня інтенсивність трафіку:  $\mu=85$  (кадрів/с)

середня довжина повідомлення:  $l=600$  байт;

вимоги до затримки передачі пакету –  $\leq 5$  мс.

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускнуною здатністю 1000Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку  $\mu=85$  (кадрів/с), а середня довжина повідомлення – 600 байт.

Розрахуємо пропускну здатність мережі на рівні доступу припускаючи, що послугами одночасно користуються 100% користувачів.

$$P_{p.d} = \mu \cdot l \cdot n \cdot 8 = 85 \cdot 600 \cdot 45 \cdot 8 = 18,36 \text{ (Мбіт/с), де}$$

$n$ - кількість користувачів.

Отримані результати показують що характеристик та пропускну спроможності достатньо.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускну здатністю 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 1000\ 000\ 000 / (600 \cdot 8) = 208334 \text{ пакетів/с}$$

Оскільки кожне джерело виробляє в середньому 85 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

$$N = 208334 / 85 = 2451 \text{ джерело.}$$

Що задовольняє нашу мережу на 45 ПК.

Кожен 45 ПК посилає потік заявок з інтенсивністю 85 кадрів/с.

Інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda = N \cdot \mu = 45 \cdot 85 = 3825 \text{ (пакетів/с)}$$

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

$$\rho = \lambda / \mu_{вих} = 3825 / 208334 = 0,02$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \rho / (1 - \rho) = 0,02 / (1 - 0,02) = 0,02$$

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

$$T=1/((\mu-\lambda))=1/(208334-3825)=4.8 \cdot 10^{-6} \text{ с}$$

Середня довжина черги:

$$L_{\text{чер}}=\rho^2/(1-\rho)= [0,02^2/(1-0,02)=0,0004$$

Розрахунки показують, що наша мережа недовантажена. З одного боку можна замінити обрані апаратні засоби на більш дешеві, чим знизити вартість самої мережі. Але якщо використовувати застаріле обладнання то мережа не зможе виконувати сучасні функції, які роблять її сучасною і ефективною.

## 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

### 4.1 Аналітичний огляд стану електронної комерції в Україні

Під електронною комерцією розуміється така форма комерції, коли вибір і замовлення товару чи послуг виконуються через комп'ютерні мережі, а оплата – шляхом використання електронних документів та платіжних засобів (картки, електронні чеки, електронні гроші).

За кілька років торгівля в Інтернеті стала одним з наймогутніших сегментів національних економік промислово-розвинутих країн, особливо – у США. Суспільство переходить на якісно новий етап розвитку, де визначальну роль відіграє інформація.

Електронна комерція переживає нині швидке зростання та поширення у всьому світі. В Україні також починають налагоджуватись необхідні для цього умови, що дозволяють організовувати успішну торгівлю в мережі Інтернет.

Оскільки рівень розвитку країни оцінюється рівнем її інформатизації, а розширення інформаційних технологій і Інтернет безпосередньо впливають на економічне зростання країни, то важливою метою для України є швидке входження в систему міжнародної електронної торгівлі і підтримка Інтернет-економіки у всіх сферах економічної діяльності.

Таким чином, викладені факти дозволяють зробити висновок, що електронна комерція стане одним з наймогутніших сегментів національної економіки не тільки США, але й багатьох країн світу, що з успіхом впроваджують нові технології в усі сфери життєдіяльності суспільства.

Але при швидкому розвитку електронної комерції постає важливе питання необхідності забезпечення безпеки інформаційної та інтелектуальної власності.

На даний час такий вид електронної комерції як організація Інтернет-магазинів, що працюють з матеріальними товарами, досить розвинений та

розповсюджений. Але у випадку, коли товар є нематеріальним, тобто це - інформація або об'єкти права інтелектуальної власності, забезпечення безпечної взаємодії стає набагато складнішим. Необхідно підкреслити, що оскільки інформація стала новим видом товару в інформаційному суспільстві, придбання об'єктів права інтелектуальної власності з кожним роком відбувається все частіше. Це означає, що необхідно якнайшвидше розробити протокол взаємодії суб'єктів електронної комерції, предметом якої є об'єкти права інтелектуальної власності. На сьогоднішній день таких протоколів не існує, а інформаційні товари обробляються за схемами, розробленими для матеріальної продукції, що не є ані доцільним, ані безпечним. Тому в даній магістерській дипломній роботі запропоновано варіант протоколу, що усуває недоліки існуючих альтернативних схем і спрямований на підвищення безпеки інформаційної та інтелектуальної власності.

Необхідно зазначити, що в Україні (та в інших країнах) існує категорія людей, яка постійно взаємодіє в сфері електронної комерції, предметом якої є об'єкти права інтелектуальної власності, але вони не мають надійний протокол взаємодії між сторонами. Ця категорія людей називається «фрілансерами», і їх діяльність полягає в тому, що вони постійно взаємодіють з різними замовниками, виконуючи окремі інформаційні послуги. З кожним днем кількість фрілансерів зростає. Оскільки не розроблені протоколи, що забезпечать безпеку таких взаємодій, існують постійні ризики як для замовників, так і для виконавців.

#### **4.2 Довіра у сфері електронних комунікацій**

Оскільки "електронні" відносини стають все більш звичними для мільйонів людей - з'являються можливості здійснювати закупівлі в магазинах електронної торгівлі, користуватися системами електронних банківських розрахунків, укласти електронні договори, а звідси – значення довіри в сфері електронних комунікацій неухильно зростає.

Зрозуміло, що неможливо уникнути проблем безпеки в сфері електронних комунікацій, але, на додаток до технологій захисту, можна знайти рішення, здатне зменшити ризики. Це рішення також відомо як «довіра». Довіра у сфері електронних комунікацій не обмежується довірою до захищених комп'ютерних систем - адже безпека комп'ютерної системи залежить не тільки від надійної операційної системи, але і від фізичних засобів захисту, від кваліфікації та надійності персоналу тощо.

Критеріями оцінки ступеня довіри до будь-яких компаній-виробників товарів і послуг одного рівня виступають ключові елементи довіри: передбачуваність, ресурси і невизначеність[11].

Передбачуваність, тобто здатність постачальника послуг постійно видавати очікуваний (позитивний) результат, дозволяє покупцю послуг не підтримувати весь час високий рівень пильності. Чим більше передбачуваний рівень безпеки, сервісу та якості послуг постачальника, тим легше покупцеві їх придбати.

Наступний елемент довіри – ресурси (фізичні або інформаційні), а точніше ризики їх втрати. Чим більше ризики, тим вище вимоги до довіри. Вимоги до довіри також збільшуються, коли є невизначеність у можливості перевірити операцію або результат. Якщо вся інформація про сторони і угоди відома, то необхідність у довірі істотно зменшується, однак для більшості угод характерна суттєва частка невизначеності.

Один з найпростіших, але не найефективніших методів встановлення довіри у сфері електронних транзакцій полягає у використанні прозорих політик довіри. Політики довіри повинні забезпечувати:

- конфіденційність. Політики конфіденційності розробляються для того, щоб користувачі правильно розуміли, як дана компанія буде поводитися з тією персональною та діловою інформацією, яку вони їй надають. Опублікована на веб-сайті компанії політика конфіденційності пояснює правила використання персональних даних і сприяє встановленню



контакту з користувачами. Користувачі повинні ознайомитися з цією політикою й підтвердити свою згоду із зазначеними правилами;

- коректне використання інформації. Інший аспект політик довіри - коректне використання інформації. Це стосується ситуацій, коли персональна інформація може використовуватися не в інтересах людини, а, наприклад, для оцінки його фінансових можливостей як потенційного покупця. На даний час деякі компанії практикують відбір та класифікацію споживачів певних товарів і послуг, а потім продають цю інформацію іншим компаніям. Подібна практика призводить до того, що люди починають отримувати поштою небажані повідомлення рекламного характеру, їх змушують відповідати на телефонні дзвінки, їх намагаються залучити в якості потенційних клієнтів кредитних карткових систем тощо;

- реагування в разі порушення довіри. Політика довіри повинна пропонувати певні фінансові гарантії, тобто страхувати користувача, на той випадок, коли неможливо забезпечити повний захист його ресурсів. Досить часто в політиках міститься твердження про те, що суперечки щодо порушення конфіденційності розглядаються в арбітражному суді. Слід враховувати, що арбітражний розгляд має набагато менш серйозні наслідки для сторони, яка порушила політику довіри, ніж судовий. Очевидно, що в штаті великих компаній, зацікавлених у підтримці відносин довіри, повинен бути присутнім адміністратор інформаційної безпеки або особа, відповідальна за конфіденційність персональних даних;

- внутрішні механізми гарантування безперервності довіри. Політика довіри повинна розкривати внутрішні механізми довіри і демонструвати, що довіра є важливою складовою частиною ділових операцій;

- згоду користувачів. Політика довіри повинна передбачати механізм отримання згоди користувачів, він зазвичай називається участю. Часто компанії автоматично припускають згоду користувача на участь, тим

самим перекладаючи на нього відповідальність за можливі наслідки порушення конфіденційності.

Концепції довіри підтримують наступні технології:

- аналіз вразливості - зниження кількості атак на ресурси, підвищення передбачуваності і зменшення невизначеності якості послуг;
- онлайн-послуги депонування - забезпечення захисту ресурсів в умовах невизначеності взаємодії з невідомою стороною. Досягнення передбачуваності на основі історії транзакцій депонування;
- міжмережеві екрани - захист ресурсів від онлайн-атак.

Оскільки в даній дипломній роботі не розглядаються проблеми веб-атак на ресурси, а основна увага приділяється дослідженням протоколу захисту конфіденційності інформації, що базується на інфраструктурах відкритих ключів, тобто забезпеченню неможливості некоректної поведінки з боку як замовника, так і виконавця, далі в роботі буде розглянуто безпеку такої технології концепції довіри, як онлайн-послуги депонування, а саме – використання третьої довірчої сторони.

### **4.3 Аналітичний огляд структури протоколу «Escrow»**

Наразі для безпечного придбання об'єктів права інтелектуальної власності в електронному середовищі використовується протокол, який частково вирішує зазначені проблеми та має назву «Escrow». Існують російські аналоги з такою ж самою схемою реалізації, вони мають назви «Угода без ризиків» та «Безпечна угода». Суттєвим недоліком протоколу є те, що він був сформований для безпечних взаємодій з матеріальними об'єктами, а для взаємодій з об'єктами права інтелектуальної власності зазнав лише незначних змін, що зменшує захищеність конфіденційної інформації під час взаємодії між відправником та утримувачем. Також більшість сервісів типу «Угода без ризиків» та «Безпечна угода». Це означає, що протоколи, які забезпечують безпеку угод, що стосуються конфіденційної інформації, розроблені в Україні.

В зазначеному протоколі (рис. 1.4) визначено: Замовник (З), Виконавець (В), технічне завдання (ТЗ), третя довірча сторона (ТДС). На рис. 5.2 та 5.3 зображено протокол за допомогою мови візуального програмування UML. На рис. 5.2 наведено схему, де в результаті виконання протоколу отримано позитивний результат, на рис. 5.3 – негативний результат.

Основним недоліком системи є те, що Виконавець має відправити для перевірки виконане завдання третій довірчій стороні, що порушує право Виконавця на збереження конфіденційності інформації. Під впливом людського фактору власники сервісу третьої довірчої сторони можуть використовувати отриманий об'єкт права інтелектуальної власності в своїх інтересах, а не тільки для збереження та звітності. Рішенням цієї проблеми є використання інфраструктур відкритих ключів з метою підвищення конфіденційності інформації, що передається.

#### **4.4 Особливості використовуваного протоколу**

Основне призначення електронної комерції – надати можливість покупцям вибирати, оформляти замовлення та здійснювати закупівлі товарів, отримувати послуги в будь-який час за допомогою мереж загального користування, а саме – мережі Інтернет. У попередніх підрозділах показано, що існує потреба в підвищенні рівня безпеки системи підтримки електронної комерції.

На шляху реалізації альтернативної системи, що підвищує захищеність взаємодій з об'єктами права інтелектуальної власності, постає багато проблем. Основною проблемою є джерело довіри системи. Очевидно, що більшість сервісів, що підтримують електронну комерцію, є приватними системами. Це означає, що існує велика ймовірність впливу людського фактору на процес обробки конфіденційної інформації.

Переважає більшість систем електронної комерції, а тим більше – великі іноземні системи, що забезпечують достатній рівень захищеності користувачів, є закритими системами. Це, по-перше, не захищає користувачів

від ризиків атаки з боку власника або оператора такої системи (з використанням «люків» або інших засобів зменшення стійкості захисту користувача в системі, які відомі тільки власникам або розробникам системи).

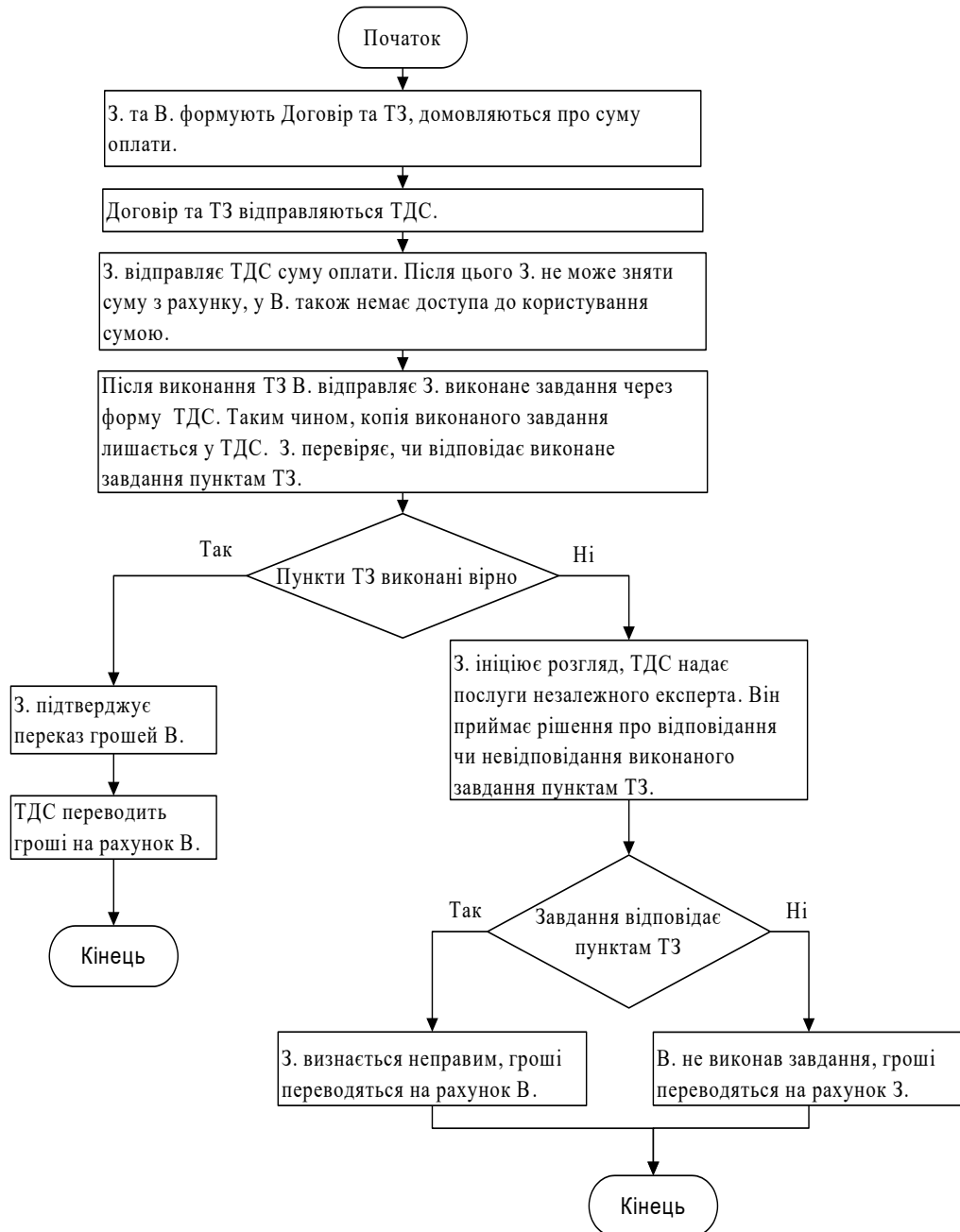


Рисунок 4.1 – Протокол системи «Escrow»



Рисунок 4.2 – Схема протоколу «Escrow», UML (позитивний результат)

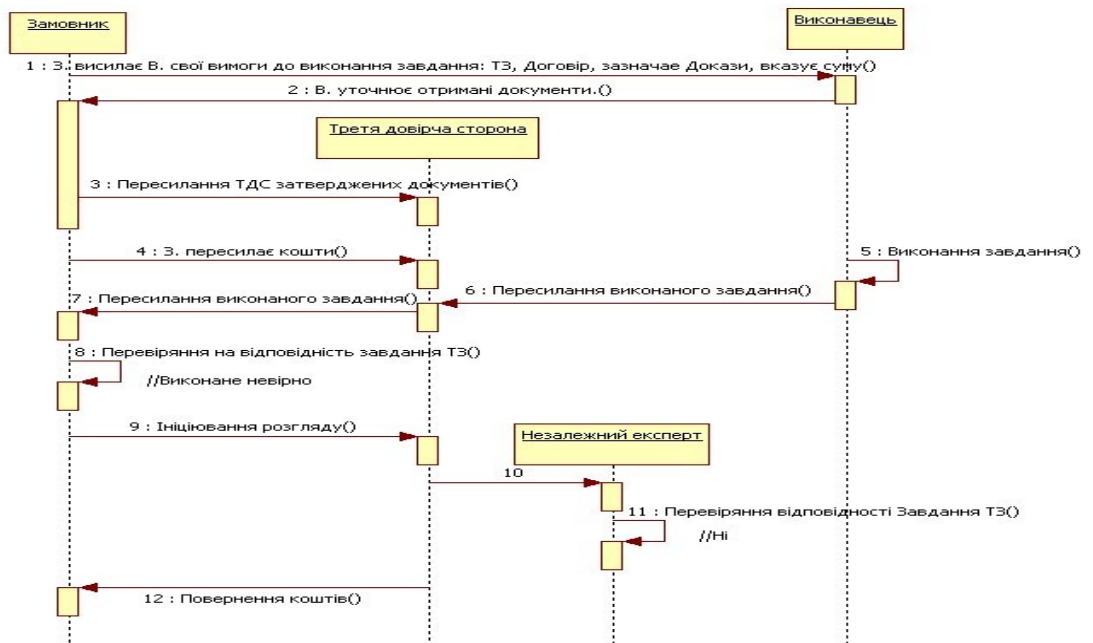


Рисунок 4.3 – Схема протоколу «Escrow», UML (негативний результат)

По-друге, це фактично унеможлиблює створення аналогічної системи з використанням чужого досвіду побудови.

Одним з надійних засобів рішення цієї проблеми є використання інфраструктур відкритих ключів з метою підвищення конфіденційності інформації, що передається. Такий підхід до організації електронної комерції надасть змогу підвищити рівень захисту інформації і зменшити ризики.

Оскільки в Україні ще не існує протоколів електронної комерції, розроблених для взаємодій з об'єктами права інтелектуальної власності, а протоколи, що зараз використовуються в цій сфері, розроблялися для взаємодій з матеріальними носіями інформації, виникла проблема неможливості забезпечення конфіденційності об'єктів права інтелектуальної власності. Вирішити цю проблему можна, імплементуючи в існуючі системи функції використання інфраструктур відкритих ключів (асиметричне шифрування за допомогою сертифікатів ІВК). Такий протокол має мінімізувати вплив людського фактору при обробці конфіденційної інформації.

## ВИСНОВКИ

Кваліфікаційна робота виконана відповідно до теми. В роботі розроблений проект корпоративної комп'ютерної мережі, яка складається з 5 локальних мереж.

Відповідно до спеціальності темою роботи є розробка корпоративної комп'ютерної мережі.

Проаналізовано організаційні особливості сучасних торгівельних мереж. Показано особливості інформаційного середовища в якому працюють торгівельні мережі.

Розроблено технічні вимоги та проект комп'ютерної системи підприємства. Комплектуючі, мережеві технічні засоби алгоритми, програмні продукти та методи обрано виходячи з сучасних швидкісних характеристик та можливостей розвитку та модернізації інформаційної системи.

У пакеті Cisco Packet Tracer розроблена модель мережі, перевірена її працездатність та розрахунок налаштувань і адресації. Розраховані параметри трафіку.

Як компонент системи розглянуто удосконалення протоколу «Escrow» системи електронної комерції .

## ПЕРЕЛІК ПОСИЛАНЬ

1. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж :[навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
2. Жуков, І. А. Комп'ютерні мережі та технології : навч. посіб./І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.
3. Аналоговые и цифровые системы видеонаблюдения (Електрон. ресурс)/Спосіб доступу:URL:<http://elites-montage.com.ua/svanalog.php>. - Загол. з екрана.
4. Формати відеоспостереження (Електрон. ресурс) / Спосіб доступу: URL: <http://spec.prom.ua/a37913-klassifikatsiya-formatov-razresheniya.html> – Загол. з екрана.
5. Закон України “Про електронний цифровий підпис”, 2003 – 10 с.
6. IP Калькулятор [Електронний ресурс] – Режим доступа : URL : <http://ip-calculator.ru/>. – Загол. з екрана.
7. VLSM Calculator – калькулятор подсетей с маской переменной длины [Электронный ресурс]. – Режим доступа:URL:<http://www.vlsm-calc.net/>. – Загол. з екрана.
8. Воробьёва Н.И., Корнейчук В.И., Савчук Е.В. Надёжность компьютерных систем. – К.: «Корнійчук», 2002. – 144 с.
9. Мережеве обладнання [Электронный ресурс] – Режим доступа : URL : [https://elmir.ua/routers/router\\_zyxel\\_sbg5500-a.html](https://elmir.ua/routers/router_zyxel_sbg5500-a.html). – Загол. з екрану.
- 10.Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи (Електрон. ресурс) / Спосіб доступу: URL: <http://www.txnet.com/ekranuvanna-servernih-primisen> – Загол. з екрана.
- 11.Баня Е.Н. Компьютерные сети. – К.: Світ, 1999. – 112 с.



12. Джеймс Челлис Основы построения сетей: Учебное пособие для специалистов MCSE 1.0. – СПб.: Питер, 1997. – 326 с.
13. Microsoft Corporation. Принципы проектирования и разработки программного обеспечения. Учебный курс MSCD/ Пер. с англ. – М., 2002. – 736 с.
14. Розробка програмного забезпечення комп'ютерних систем. Програмування [Текст]: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова. – 2-ге вид., випр. – Д.: Національний гірничий університет, 2011. – 222 с.
15. Цвіркун Л.І. Глобальні комп'ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с.
16. Комп'ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп'ютерна інженерія / Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.

## ДОДАТОК А

Текст програми налаштування мережі комп'ютерної системи

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

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ**

Текст програми

804.02070743.23022-01 12 01

Листів 9

Дніпро

2023

## АНОТАЦІЯ

Дана програма містить в собі частину програмного коду програмування та налаштування компонентів мережі комп'ютерної системи.

Програма призначена для забезпечення налаштування, протоколу маршрутизації NAT комп'ютерної системи.

**ЗМІСТ**

	Стор.
1. Скрипт налаштування ISP	5
2. Скрипт налаштування Router0	5
3. Скрипт налаштування Router1	6
4. Скрипт налаштування Router2	7
5. Скрипт налаштування Router3	8
6. Скрипт налаштування Router4	8

## 1. Скрипт налаштування ISP

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!hostname Router  
ip cef  
no ipv6 cef  
license udi pid CISCO2911/K9 sn FTX1524ZI9T-  
spanning-tree mode pvst  
interface GigabitEthernet0/0  
ip address 10.0.2.21 255.255.255.252  
duplex auto  
speed auto  
interface GigabitEthernet0/1  
ip address 10.0.2.1 255.255.255.252  
duplex auto  
speed auto  
interface GigabitEthernet0/2  
ip address 209.165.201.5 255.255.255.252  
duplex auto  
speed auto  
interface Vlan1  
no ip address  
shutdown  
ip classless  
ip flow-export version 9  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
end
```

## 2. Скрипт налаштування Router0

```
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
hostname Router  
ip cef  
no ipv6 cef
```

```
license udi pid CISCO2911/K9 sn FTX1524THM8-  
spanning-tree mode pvst  
interface GigabitEthernet0/0  
ip address 172.23.224.65 255.255.255.224  
duplex auto  
speed auto  
interface GigabitEthernet0/1  
ip address 10.0.2.22 255.255.255.252  
duplex auto  
speed auto  
interface GigabitEthernet0/2  
no ip address  
duplex auto  
speed auto  
shutdown  
interface Vlan1  
no ip address  
shutdown  
ip classless  
ip flow-export version 9  
line con 0  
line aux 0  
line vty 0 4  
login  
end
```

### **3. Скрипт налаштування Router1**

```
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
hostname Router  
no ip cef  
no ipv6 cef  
license udi pid CISCO2911/K9 sn FTX1524M69D-  
spanning-tree mode pvst  
interface GigabitEthernet0/0  
ip address 172.23.224.129 255.255.255.240  
duplex auto  
speed auto  
interface GigabitEthernet0/1  
ip address 10.0.2.9 255.255.255.252  
duplex auto  
speed auto
```

```
interface GigabitEthernet0/2
ip address 10.0.2.14 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/3/0
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/1
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/2
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/3
switchport mode access
switchport nonegotiate
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

#### **4. Скрипт налаштування Router2**

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15241J49-
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.23.224.113 255.255.255.248
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 10.0.2.18 255.255.255.252
duplex auto
```



```
speed auto
interface GigabitEthernet0/2
ip address 10.0.2.26 255.255.255.252
duplex auto
speed auto
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

### **5. Скрипт налаштування Router3**

```
version 15.1

no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Router

no ip cef
no ipv6 cef

license udi pid CISCO2911/K9 sn FTX1524T0SG-

spanning-tree mode pvst

interface GigabitEthernet0/0
ip address 172.23.224.1 255.255.255.192
duplex auto
speed auto

interface GigabitEthernet0/1
ip address 10.0.2.2 255.255.255.252
duplex auto
speed auto

interface GigabitEthernet0/2
ip address 10.0.2.5 255.255.255.252
duplex auto
speed auto

interface FastEthernet0/3/0
```

```
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/1
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/2
switchport mode access
switchport nonegotiate
interface FastEthernet0/3/3
switchport mode access
switchport nonegotiate
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

#### **6. Скрипт налаштування Router4**

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524LB6L-
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 10.0.2.6 255.255.255.252
```

```
duplex auto
speed auto
interface GigabitEthernet0/1
ip address 10.0.2.25 255.255.255.252
duplex auto
speed auto
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```