Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедраі нформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи бакалавра

студента Приходько Андрія Андрійовича
(ПІБ)

академічної групи 123-17ск-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: *"Комп'ютерна система відеонагляду ТОВ «Вітязь» з детальним опрацюванням побудови, налаштуваннята безпеки корпоративної мережі"*

Виконавець: студент 3 курсу, групи 123-17ск-1 _____ Приходько А.А.
(підпис) (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.			
Спеціальна частина	ас. Панферова Я.В.			
Економічний розділ	ст.в. Яремчук І.О.			
Охорона праці	доц. Іконніков М.Ю.			
Рецензент				
Нормоконтролер	Проф.Цвіркун Л.І.			

Дніпро
2020

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
Інформаційних систем та технологій
проф. Гнатушенко В.В.

_____
"27" січня 2020 р.

ЗАВДАННЯ
на кваліфікаційну роботу
бакалавра
(назва освітньо-кваліфікаційного рівня)

студенту групи *123-17ск-1 ПриходькоАндрію Андрійовичу*
(група) (прізвище, ім'я та по батькові)

Тема дипломної роботи*"Комп'ютерна система відеонагляду ТОВ «Вітязь» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"*

затверджена наказом ректора НТУ "Дніпровська політехніка"
від «26»05 2020 р. № 275-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	*На основі матеріалів виробничих практик, інших науково-технічних джерел обгрунтувати необхідність модернізації комп'ютерної системи з детальною розробкою комп'ютерної мережі та системи відеонагляду.*	*15.03.2020 р.*
Технічні вимоги до системи керування	*На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної мережі.*	*01.04.2020 р.*
Спеціальна частина	*Розв'язати завдання з розробки комп'ютерної мережі ТОВ «Вітязь»з опрацюванням побудови та налаштування з урахуванням IP відеокамер.*	*15.05.2020 р.*
Графічна частина	*Графічні результати розробки системи подати у вигляді рисунків електричних схем та інших креслень на 10 арк. формату А4.*	*25.05.2020 р.*

Завдання видав, кер. роботи доц. Шедловський І.А.
(підпис)

Завдання прийняв до виконання Приходько А.А.
(підпис)

Дата видачі завдання *01.02.2020 р.*

Термін подання дипломної роботи до ДЕК *01.06.2020 р.*

РЕФЕРАТ

Пояснювальна записка: 85 с., 19 рис., 6 табл., 1 додаток, 28 джерел.

Об'єкт розробки: система відео нагляду длязабезпечення ефективного функціонування ТОВ «Вітязь» з опрацюванням побудови та налаштувань комп'ютерної мережі.

Мета: створення комп'ютерної мережі для забезпечення сучасними засобами IT комунікації та використання сучасних методів управління з використанням IP відеокамер для удосконалення системи прийняття рішень на базі алгоритмів відеоаналітики.

Розроблена система забезпечує можливість гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову системи оперативного управліннята збору і підготовки статистичної і економічної інформації.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

- безперервний збірта збереження інформації;
- автоматизовану обробку і перенапрвленнявідео інформації в базу даних, захист приміщень ТОВ «Вітязь» від несанкціонованого доступу;
- швидку і якісну обробку запитів;

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

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

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

СИСТЕМА, КОМПЮТЕРНА МЕРЕЖА, IP ВІДЕОНАГЛЯД, НАЛАШТУВАННЯ

ЗМІСТ

ПЕРЕЛІК УМОВНХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

СРМ–обсяг продажів на тисячу відвідувачів;

SSF – число продажів на одиницю площі;

АРМ–автоматизоване робоче місце;

КІСП – комп’ютерна інформаційна система підприємства;

ЛОМ – локальна обчислювальна мережа;

ЦП – цифровий підпис;

ВСТУП

Практика свідчить, що об’єкти управління при ринковій економіці, коли діє широка конкуренція, не можуть весь час ефективно функціонувати, якщо сучасні засоби електронної обчислювальної та інформаційної техніки не використовуватимуться в усіх процесах оперативного збирання та обробки інформації як на об’єктах управління, так і під час обміну інформацією між суб’єктами такої економіки.

В кваліфікаційній роботі розроблена комп’ютерна система відеонагляду ТОВ «Вітязь» з опрацюванням побудови та налаштувань комп’ютерної мережі. Підприємство розташоване в двоповерховій будівлі. Контрольована зона обмежена стінами торгівельного залу першого поверху та другим поверхом.

Встановлення мережевої камери (камер) вирішує чимало проблем для підприємств бізнесу та торгівлі. Організація якісної системи відеоспостереження в сукупності з професійною аналітикою - це дієвий метод безпеки щодо попередження крадіжок в роздрібних мережах торгівлі, який досить ефективний, для виявлення недобросовісних клієнтів, співробітників і постачальників, з якими доводиться працювати щодня.

Слід додатково зазначити, що наявність попереджувальних табличок, про відеоспостереження на об'єкті - обов'язкова умова, тому, що, згідно з Законодавства України, використання камер прихованого спостереження без відома на те осіб, щодо яких проводиться спостереження, заборонено і переслідується законом.

Найчастіше, коли зачіпається тема відеоспостереження на підприємствах торгівлі, розваг, громадського харчування, то все зводитися тільки до можливостей організації так званих відео-POS систем Проте, можна виділити групу властивостей сучасних систем відеоспостереження, затребуваних в даному секторі бізнесу. До цього переліку входять:

відео-POS системи та інтеграція з ПЗ автоматизації торгівлі; різноманітні можливості віддаленого доступу до системи

відеоспостереження; технології інтеграції з типовими елементами загальної системи безпеки; технології інтеграції зі спеціальними і, в першу чергу, антікражних системами; спеціальні модулі інтелектуального аналізу відеозображення.

Дляорганізації відео POS систем використовується спеціальні технології синхронізації відеоданих з подіями і даними касових терміналів або всієї фронт - офісної програми в цілому. Під абревіатурою POS (PointofSale) розуміється касовий термінал і зона навколо нього, а під фронт - офісної програмою - частина програмного комплексу автоматизації підприємства торгівлі, що відповідає за роботу з касовими терміналами і пристроями касової зони.

При використанні технології POS-Інтелект, за рахунок розширених можливостей самого «Інтелекту», користувач має потужний сервіс в аналітиці та отриманні різноманітних звітів, а також є можливість скористатися широким вибором інших інтегрованих технологій і систем;

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

Звичний спосіб здійснення покупок в магазинах поступово змінюється. З ростом популярності онлайн-магазинів люди можуть отримати все, що їм подобається, прямо до своїх дверей. Тому головна причина, поякій вони відвідують торгові центри, - це враження.

Торгові центри - зараз і в майбутньому - це більше, ніж просто шопінг. Торгові центри - це атмосфера, в якій людям приємно зустрічатися з друзями і спілкуватися з представниками їх улюблених брендів. Відвідувачі торгових центрів розраховують на те, що їх досвід відвідування магазинів оффлайн буде більш цікавим, ніж здійснення покупок в Інтернеті. Ця тенденція поширюється по всьомусвіту, але азіатські торговельні центри просунулися далі інших в задоволенні цих зростаючих потреб своїх клієнтів.

Відповідно до звіту дослідницької компанії AT Kearney названому «Майбутнє торгових центрів», адміністраторам торгових центрів буде потрібно освоїти два набори технологій для забезпечення належного рівня обслуговування своїх клієнтів:

Технології, які споживачі використовують в своєму повсякденному житті для спілкування та ведення комерційної діяльності, такі як мобільні телефони, планшети і встановлені в них програми.

Технології, які підприємства вже використовують і будуть використовувати для ідентифікації покупців, розрахунку часу очікування, аналізу поведінки, спілкування з клієнтами та підвищення ефективності своєї діяльності, що стосується мерчендайзингу, маркетингу, реклами і просування [1].

Це апаратно-програмне забезпечення або технологія, що використовують методи комп'ютерного зору для автоматизованого збору даних на підставі аналізу потокового відео (відеоаналізу). Відеоаналітіка спирається на алгоритми обробки зображення і розпізнавання образів, що дозволяють аналізувати відео без прямої участі людини. Відеоаналітіка

використовується в складі інтелектуальних систем відеоспостереження (CCTV, охоронного телебачення), управління бізнесом (business intelligence, BI) і відеопошуку.

Виявлення об'єктів (object detection). Як правило, виявлення об'єктів в полі зору камери проводитися за допомогою відеодетектора руху. Основна відмінність відеоаналітики від ІЧ-датчиків руху полягає в можливості локалізації (виділення) та незалежного аналізу відразу декількох об'єктів. Якщо рух не є достатньою ознакою для локалізації об'єкта в кадрі, то виявлення може проводитися за допомогою шаблонів. Наприклад, виявлення осіб людей, номерних знаків автомобілів або виявлення малорухомих морських цілей.

Стеження за об'єктами (object tracking). Алгоритми стеження (супроводу) дозволяють отримати приватну траєкторію руху об'єкта як в поле зору однієї камери, так і узагальнену траєкторію за даними відразу декількох камер. Стеження необхідно, щоб проаналізувати поведінку об'єкта по його траєкторії, наприклад, визначити рух людини проти потоку або рух з підвищеною швидкістю. Крім цього, стеження необхідно для виключення повторних спрацьовувань систем відеоаналітики на одні і ті ж об'єкти. Професійні системи працюють за правилом «один тривожний об'єкт - одне спрацьовування» для досягнення високої продуктивності оператора.

Класифікація об'єктів (object classification). Деякі системи відеоаналітики класифікують об'єкти для фільтрації оперативних повідомлень або результатів пошуку. Наприклад, типовий класифікатор об'єктів, використовуючи ознаки форми і абсолютні розміри, розподіляє об'єкти на групи: людина, група людей, транспортний засіб. Більш складні класифікатори в системах відеоаналітики можуть визначити стать або поворотну групу людини.

Ідентифікація об'єктів (object identification). Ідентифікація об'єктів є найбільш складним компонентом систем відеоаналітики. Сучасні системи дозволяють ідентифікувати людей за біометричними ознаками особи

аботранспортні засоби - за номерними знаками. Ідентифікація може бути реалізована за допомогою додаткових коштів за рамками відеоаналітики: на основі відбитків пальців, банківської карти, квитка, пропуску або ідентифікатора мобільного пристрою.

До недавніх пір алгоритми відеоаналітики застосовувалися в основному для детектування подій, підрахунку відвідувачів, розпізнавання небезпечних предметів і ідентифікації осіб з метою забезпечення безпеки на різних об'єктах. Сучасні розробки в області відеоаналітики здатні вирішувати великий спектр комерційних завдань. Алгоритми можуть здійснювати збір та аналіз важливою маркетингової інформації в режимі реального часу (підрахунок людей і транспорту, моніторинг активності людей в окремих зонах і т.д.). У міру розвитку технологій аналізу великих даних інформація, яка надходить від систем відеоспостереження, стає все більш цінною і починає активно використовуватися бізнесом [4].

Функції системи відеоаналітики.

• Підрахунок людей і транспорту, який здійснюється в режимі реального часу.

• Збір та аналіз кількісних даних, зібраних в результаті роботи алгоритмів за підрахунком.

Підрахунок людей в комерційних цілях проводиться для розрахунку декількох важливих показників ефективності бізнесу:.

• CPM (Cost Per Mile або Cost Per Thousand - обсягпродажівнатисячувідвідувачів).

• SSF (Sales Per Square Foot або Sales Per Unit Area - числопродажівнаодиницюплощі).

Можливості для бізнесу

• Прогнозування продажів на основі даних про реальний поток відвідувачів/покупців

• Оцінка ефективності бізнесу, розрахунок коефіцієнта конверсії en:Conversion rate на підставі статистичних даних про відвідуваність об'єкта

• Прив'язка мотиваційної системи співробітників до коефіцієнта конверсії en: Conversion rate

• Аналіз якості використання потужностей: торговельної площі, роботи персоналу

• Оцінка ефективності рекламних компаній і вкладень в PR і маркетинг на підставі даних про відвідуваність об'єкта

• Зниження витрат на персонал, коригування кількості персоналу в зміні і графіка роботи об'єкта відповідно інтенсивністю потоку відвідувачів

Основні можливості відеоаналітики для торгових центрів:

• Облік потоків відвідувачів;

• Аналіз поведінки відвідувачів;

• Аналіз черг;

• Аналіз якості обслуговування;

• Безпека;

Облік руху потоку покупців.

Точне визначення кількості відвідувачів що пройшли через головний вхід:

Визначення загальної конверсії торгового центру (за наявності інформації про загальну кількість покупок в ТЦ). Поділ напрямків потоків покупців.

Підрахунок кількості покупців в ключових зонах поділу потоку (переміщення по поверхах).

Визначення кількості покупців на кожному поверсі з урахуванням поділу по ескалаторах/ліфтів.

Аналіз послідовності дій відвідувачів.

• Чітке уявлення про потоках покупців.

• Покращення планування торгових площ, викладення товару, вітрин.

• Можливість оцінки ефективності маркетингових та рекламних вкладень.

• Можливість визначити найбільш важливі ділянки і «мертві зони».

• Оптимізація персоналу в торговому залі.

• Скорочення черг. Будь-яка компанія, що розвивається стикається з проблемою систематизації інформації та автоматизації процесів, що беруть участь в обробці цієї інформації [5].

1.1 Галузь застосування комп'ютерної системи

Компютерна система і локальна мережа підприємства повинна забезпечувати менеджмент за основним напрямком діяльності.

Основними напрямком діяльності підприємства є: роздрібна та дрібнооптова торгівля промисловими товарами.

Клієнтами ТОВ «Вітязь» є фізичні особи, приватні підприємці, фірми будь-якої форми власності і напряму діяльності, в тому числі й державні установи на всій території України, а також іноземні підприємства.

1.2 Характеристика і структура об'єкта впровадження

Підприємство розташоване в двоповерховій будівлі. Контрольована зона обмежена стінами торгівельного залу першого поверху та другим поверхом.

Відомості про будинки, будівлі та споруди, що оточують будинок, в якому знаходиться ТОВ «Вітязь» :

– житловий будинок (5 поверхів) – 15 м на північ від приміщення;
– продуктовий магазин «Вікторія» – 20 м на південь від приміщення;
– житловий будинок (9 поверхів) – 50 м на захід від приміщення;
– аптека – 60 м на схід від приміщення (Рис.1.1).

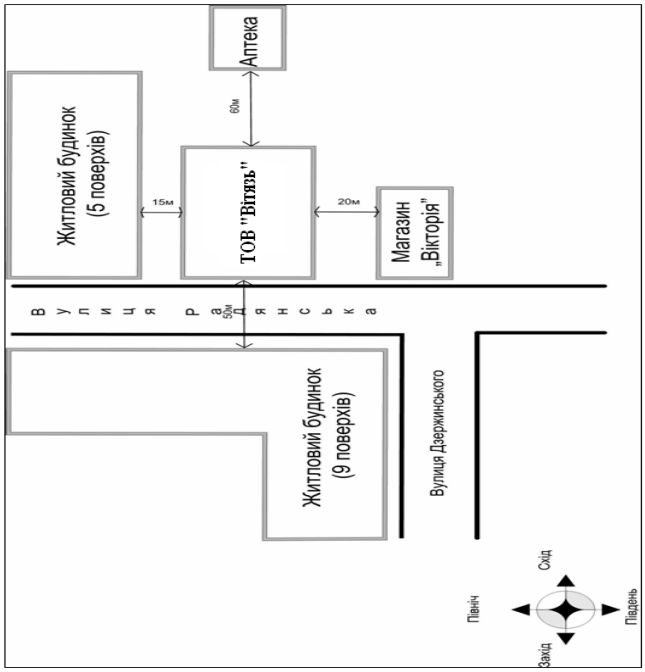

Рисунок 1.1 – Розташування будівлі ТОВ «Вітязь»

На даному підприємстві є такі приміщення (Рис.1.2, Рис.1.3):

- кабінет директора;
- кабінет заступника директора;
- приймальня;
- комерційний відділ;
- кімната охорони;
- кімната головного бухгалтера;
- кімната фінансово – економічної служби;
- кімната відпочинку;
- кімната персоналу;
- санітарний вузол;
- складські приміщення;
- торгівельний зал.

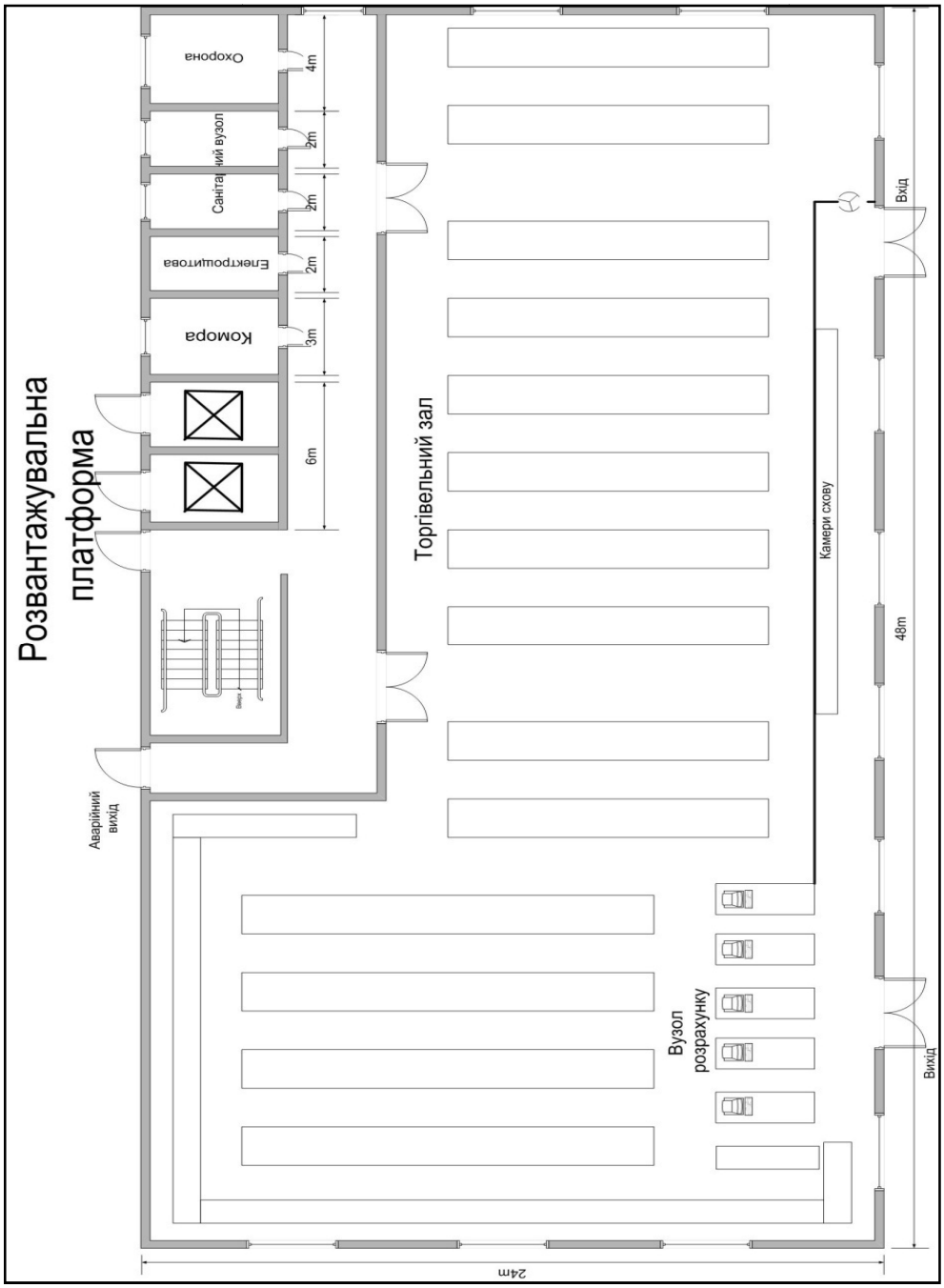

Рисунок 1.2 – План першого поверху

Стелі приміщень підвісні, виготовлені з гіпсокартону. Їх товщина складає 0,08 м. Висота від підлоги до стелі – 4 м.Вікна металопластикові. Ширина вікна – 1,9 м, висота – 1,7 м, товщина скла - 0,04 м.Вхідні двері металопластикові товщиною 0,10 м, оснащені механічним замком.

Міжкімнатні двері металопластикові товщиною 0,10 м, оснащені механічним замком.

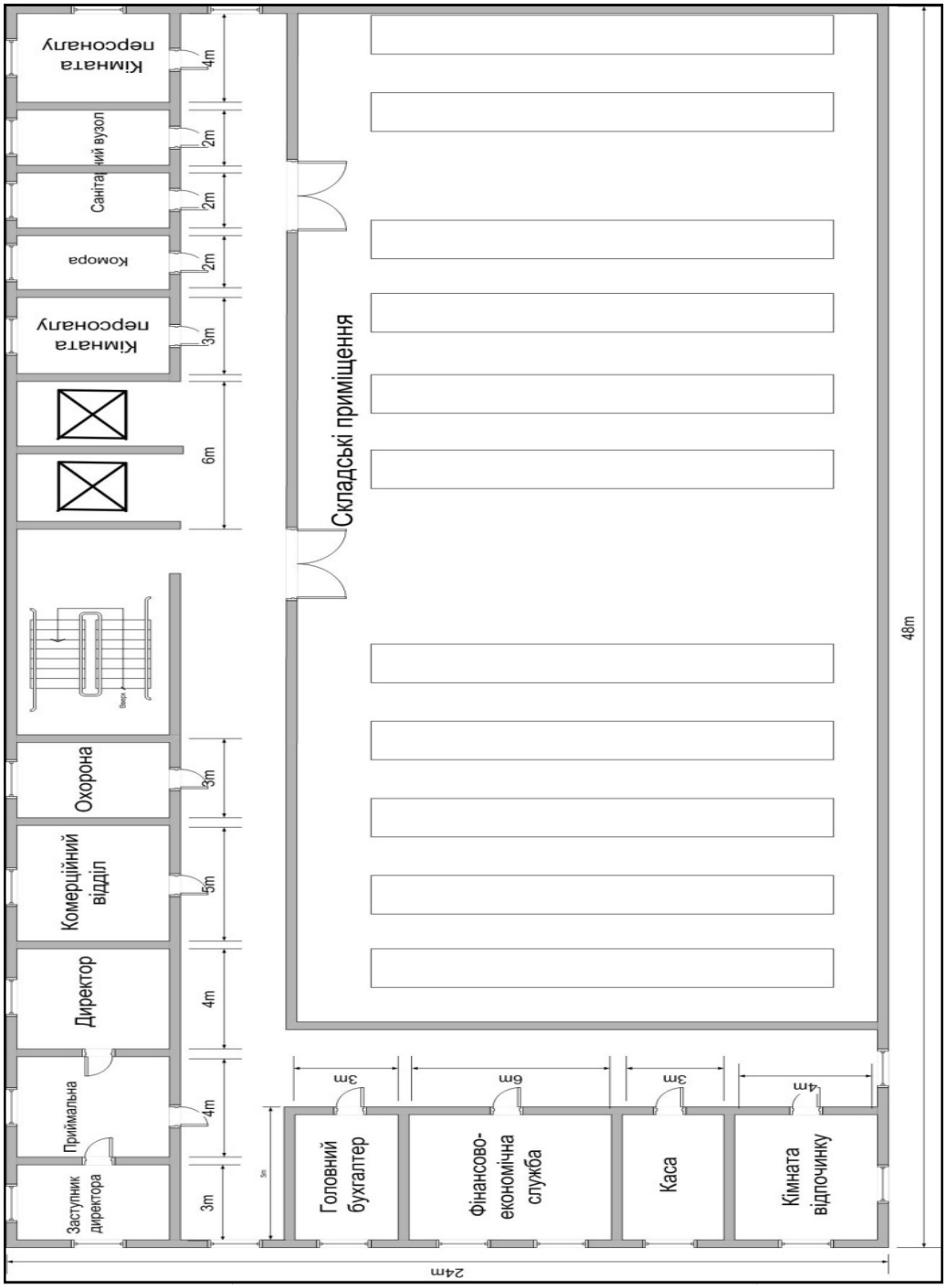

Рисунок 1.3 – План другого поверху

Загальна площа приміщення складає 2304 м².

Системи комунікацій ТОВ «Вітязь»:

– централізоване електропостачання здійснюється від трансформаторної електростанції.

– централізована система опалення;

– автономна система вентиляції;

– централізована система каналізації;

– система заземлення забезпечує заземлення всіх приладів, комп'ютерів і телефонів, присутніх на підприємстві, на загальний контур заземлення;

– телефонна лінія підключена до АТС «Укртелеком»;

– комп'ютери об'єднані в локальну мережу і мають вихід в Інтернет;

– система охоронної сигналізації, ПКП якої підключена до центрального пульта охоронного агентства.

Система відео спостереження

Система працює наступним чином: інформація з камер надходить до комутатора, з комутатора інформація надходить до сервера 17ідео спостереження.

Система ідео спостереження працює цілодобово.

1.3 Функціональні особливості системи

Компютерна система відноситься до класу фінансово-управлінських систем (малі інтегровані системи). Системаповинна гнучко настроюватися на потреби конкретного підприємства, добре інтегрувати діяльність підприємства і призначені, насамперед, для обліку й управління ресурси невиробничих компаній. Хоча у багатьох системах присутні базові можливості управління виробництвом. Як правило, вони універсальні, функціональні можливості таких систем ширші, ніж локальних[2].

Комп'ютерна інформаційна система підприємства (КІСП) це сукупність економіко-математичних методів і моделей, технічних, програмних, технологічних засобів і рішень, а також спеціалістів, призначена для обробки інформації й прийняття управлінських рішень.

Забезпечувальна частина КІСПскладається з технічного, інформаційного, математичного, організаційного, правового, ергономічного й іншого видів забезпечення.

Інформаційна система (ІС) – це система, яка організує зберігання і маніпулювання інформацією про проблемну область. Під терміном «маніпулювання» маються на увазі процедури збору, обробки, пошуку, передачі інформації, необхідної в процесі прийняття рішень в будь-якій області. Тому призначення інформаційної системи – це виробництво інформації для потреб організації в забезпеченні ефективного управління її діяльністю. ІС можна розглядати як систему управління. Як у будь-якій системі управління, в ІС існують органи управління (Рис. 1.4).

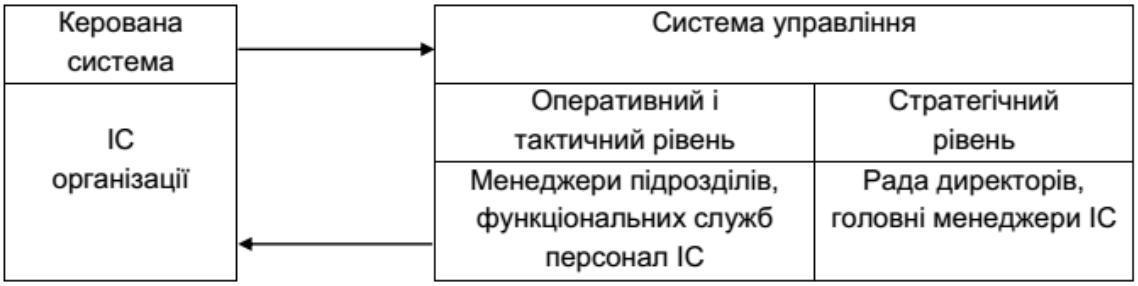

Рисунок 1.4 – Структура інформаційної системи підприємства

Повноцінне функціонування КІСП можливе лише на базі сучасної комп’ютерної мережі [3].

Програмне забезпечення призначене для управління системою контролерів, збору і обробки інформації, що надходить від них. Підключення PERCo – SYSTEM -12000 до локальних комп’ютерних мереж надає можливість створення автоматизованих робочих місць (АРМів) для різних служб:

АРМ «Адміністратор».

Забезпечує зручне і швидке управління системою: управління правами доступу користувачів, створення та робота з базами даних, підключення і зміна налаштувань апаратури;

АРМ «Охорона».

Дозволяє проводити моніторинг системи, забезпечує зручне і швидке управління всіма виконавчими пристроями (реакція на тривожні події, оперативний заборону пропуску).

АРМ «Відділ праці та заробітної плати».

Модуль обліку робочого часу дозволяє автоматизувати облік робочого часу і отримувати табель за стандартною формою.

З метою генерації звітів відпрацьованого за минулий час підтримується архів за один рік.

АРМ «Відділ кадрів».

Значно скорочує обсяг рутинної роботи, дозволяючи автоматизувати кадровий облік, оперативно вносити зміни в кадрове розклад і отримувати звіти по персоналу.

АРМ «Бюро перепусток».

Значно полегшує роботу з видачі та обліку постійних і разових перепусток, прискорює процес оформлення картки доступу у вигляді пропуску з фотографією. Фотозображення може вводитися в комп'ютер за допомогою сканера, цифрового фотоапарата або відеокамери. Нанесення зображення на карту може здійснюватися двома способами: безпосередньо на карту за допомогою спеціального принтера або на наклейки за допомогою звичайного принтера.

Модуль «відео ідентифікацією і керування доступом на віддалених об'єктах». Призначений для організації режиму відео ідентифікацією і забезпечує оперативне управління віддаленим об'єктом. При піднесенні картки до зчитувача на підконтрольному об'єкті на монітор комп'ютера виводиться еталонне зображення пред'явника пропуску з бази даних персоналу з описом його прав і його зображення, отримане від встановленої на об'єкті відеокамери. Після порівняння зображень охоронець приймає рішення – дозволити або заборонити доступ, підняти тривогу. Всі його дії і порівнювані зображення фіксуються програмою в спеціальному журналі.

Модуль «Контроль маршруту пересування».

Дає можливість контролювати роботу охорони, задаючи маршрут обходу території, послідовність відвідування об'єктів, а також інтервал часу між відвідуваннями.

Модуль «Конвертер баз даних».

Дозволяє оперативно імпортувати наявну в електронному вигляді інформацію про персонал.

Рекомендоване розташування елементів системи контролю та управлінням доступом зображено схематично у додатку З. Зчитувачі потрібно встановити на двері в таких приміщеннях:

Перший поверх:

– кабінет охорони.

– торгівельний зал.

Другий поверх:

– приймальна;

– каса;

– кімната фінансово-економічна служби;

– кімната головного бухгалтера;

– кімната комерційного відділу;

– складські приміщення;

– кімната охорони.

За системою контролю та управлінням доступом слідкують охоронники, які знаходяться в кабінеті охорони на першому та другому поверсі. В їх обов‘язки входить забезпечення безперебійної роботи системи контролю та управлінням доступом, видача карток, занесення нових користувачів до бази даних.

Таким чином на підприємстві «Вітязь» необхідно вдосконалити систему контролю та управлінням доступом.

1.4 Аналіз сучасних методик організації комп’ютерних мереж IP – відео нагляду з функцією відео аналітики

З точки зору апаратно-програмної архітектури, розрізняють наступні типи систем відеоаналітики:

Серверна відеоаналітіка (server video analytics) передбачає централізовану обробку відеоданих на сервері. Як правило, сервер аналізує відеопотоки від безлічі камер або кодерів на центральному процесорі (CPU) або на графічному процесорі (GPU). Основною перевагою серверної відеоаналітики є можливість комбінування алгоритмів відеоаналітики на одній апаратній платформі. Головний недолік серверної відеоаналітики - необхідність безперервної передачі відео від джерела відеоданих на сервер, що створює навантаження на канали зв'язку.

Вбудована відеоаналітіка (edge video analytics) реалізується безпосередньо в джерелі відеоданих, тобто в камерах в кодерах. Вбудована відеоаналітіка працює на виділеному процесорі (архітектури DSP, ASIC, FPGA, ARM або x86) пристрою і передає результати (метадані) разом з відеопотоком. Головна перевага вбудованої відеоаналітики полягає в зменшенні навантаження на канали зв'язку і на сервер обробки відеоданих. При відсутності об'єктів або подій відео не передається і не завантажує канали зв'язку, а сервер обробки не декодує стислий відео для відеоаналізу і індексування. У порівнянні з серверною відеоаналітикою, вбудована відеоаналітіка дозволяє збільшити в 10-100 разів ефективність використання каналів зв'язку і серверів.

Розподілена відеоаналітіка (distributed video analytics) є гібридним рішенням між серверною і вбудованою відеоаналітікою, в якому обробка розподілена між джерелом відеоданих і центральним устаткуванням. Наприклад, всистемі багатокамерного стеження, виявлення об'єктів проводитися в джерелі відеоданих, а зіставлення результатів між декількома джерелами - на сервері.

IP-відеоспостереження будується на базі технології Ethernet і враховує обмеження і можливості мережевих протоколів і стандартів, таких як RSTP, LinkAggregation, PoE і т.п. Класична структура ЛОМ стандарту Ethernet - це зірка. У проектах нерідко зустрічаємо каскадне підключення комутаторів.

Найчастіше це відбувається в ситуаціях, коли потрібно подолати обмеження на довжину мідного кабелю в 100 м.

Мінуси каскадного підключення - це затримка в передачі інформації, додатковий транзитний трафік для проміжних комутаторів і низька надійність. Переважною схемою є зірка. Якщо довжини міді в 100 метрів не вистачає, то слід переходити на оптику[6].

Оптимальна структура локальної мережі для IP-відеоспостереження наступна: периферійні комутатори приймають потік від камер і живлять їх по PoE, далі передають по міді або оптиці на якийсь центральний комутатор, так зване ядро мережі. До нього підключається станційне встаткування, сервери, УРМ.

Рисунок 1.5 – Узагальнена структура мережі IP - відеонагляду

Тепер, коли зрозуміло, особливості структури, слід вибрати комутатори, але перед цим необхідно визначити, які потоки ці комутатори будуть приймати і передавати.

Висновки

Метою кваліфікаційної роботи є створення проекту локальної обчислювальної мережі IP – відео нагляду товариства з обмеженою відповідальністю «Вітязь».

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

Можливим і найбільш доцільним рішенням є використання топологій мереж «Зірка».

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

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

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

2.1.1 Структура і функціонування системи

Комп'ютерна система повинна виконувати наступні функції:

Збір інформації.Повинен забезпечуватися прийом відео потоку від IP – камер що встановлені в приміщеннях підприємства та передача цих даних для подальшого аналізу та обробки.

Аналіз та обробка інформації. Комп'ютерна система повинна на підставі отриманих даних проводити їх попередню обробку і проводити аналіз з видачею результатів відповідно до закладених алгоритмів роботи.

Зберігання оперативних даних системи, даних для формування аналітичних звітів, документів системи, сформованих у процесі роботи. Ця функція повинна забезпечити періодичне резервне копіювання і збереження даних на додаткових носіях інформації.

Запис відео потоків камер проводиться на носії, що встановлені на відео сервері.Формування звітності. У комп'ютерній системі повинна забезпечуватися можливість формування різних видів звітів. Ця функція повинна забезпечувати механізми гнучкого налаштування, а також інструментарій щодо формування нових звітних форм.

Структура системи повинна забезпечувати оперативний контроль діяльності підприємств, можливість розширення, вихід до Інтернету

2.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи

Компютерна система відеонагляду повинна забезпечувати повноцінне функціонування наступних підрозділів: директора; заступника директора; комерційний відділ; охорону; головного бухгалтера; фінансово – економічну службу;

Загальна кількість робочих місць – не менше 10. Режим роботи комп'ютерної системи – цілодобово.

Компютерна система повинна забезпечувати наступні показники призначення:

обмеження доступу співробітників і відвідувачів об'єкта в приміщення, що охороняються;

часовий контроль переміщень співробітників і відвідувачів по об'єкту;

контроль над діями охорони під час чергування;

табельний облік робочого часу кожного співробітника;

фіксацію часу приходу і відходу відвідувачів;

часовий і персональний контроль відкриття внутрішніх приміщень;

реєстрацію та видачу інформації про спроби несанкціонованого проникнення в приміщення.

аналіз відеоданих відповідно до закладеного алгоритму.

Структура мережі повинна складатися з 4 під мереж LAN1 – LAN4.

Кількість вузлів: LAN1 –41 LAN2 – 24LAN3 –8LAN4 –15.

Інтенсивність трафіку $\mu = 160$ (кадрів/с).

Блок адрес - 192.168.IPn.0/21; для виділення підмережIPn = 88.

Зовнішня адреса HTTP-сервера: 209.165.200.4.

Середня довжина вихідного повідомлення в мережі – 600 байт.

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

2.1.3 Вимоги до надійності

При аварійних ситуаціях - вихід з ладу окремої відекамери не повинно приводити до втрати інформації. Перебої з електропостачанням на повинні впливати на працездатність обладнання. Необхідні резервні джерела енергії такої потужності, щоб забезпечити можливість впродовж 10 хвилин завершити роботу і зберегти дані.Для технічних пристроїв використовуються такі показники надійності, як середній час наработки на відмову, імовірність відмови, інтенсивність відмов.

Необхідно забезпечити*збереження даних*і захист їх від спотворень. Крім цього, повинна підтримуватися*узгодженість*(несуперечність) даних, наприклад, якщо для підвищення надійності на декількох файлових серверах зберігається декілька списків даних, то треба постійно забезпечувати їх ідентичність.Надійність програмного забезпечення повинна забезпечуватися за рахунок використання ліцензійних програмних продуктів [12].

2.1.4 Вимоги безпеки

Повинні бути забезпечені інженерно-технічні заходи щодо електробезпеки, щодо зменшення дії по кожному небезпечному і шкідливому фактору, існуючому на підприємстві, а також щодо пожежної безпеки.

2.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи

На етапі повного функціонування комп’ютерної системи підприємства, її обслуговування повинно забезпечуватися системним адміністратором. Ремонт системи має виконуватися спеціалістами підрядниками. Елементи системи, що вийшли з ладу повинні замінюватися новими.

2.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Захисту підлягає інформація з обмеженим доступом.Вибір запропонованих приладів повинен бути доцільним та відповідати вимогам до захисту інформації з обмеженим доступом

Загрозами безпеці інформації на підприємстві є:

– крадіжка (копіювання) інформації;

– знищення інформації;

– модифікація (спотворення) інформації;

– несанкціонований доступ до інформації;

– блокування доступу до інформації;

– заперечення дійсності інформації;

– нав'язування неправдивої інформації.

До конфіденційної інформації підприємства відноситься:

– інформація про плани підприємства;

– інформація про фінанси підприємства;

– договори про надання клієнтам послуг;

– інформація про партнерів підприємства;

– персональні дані співробітників;

– трудові договори співробітників;

– внутрішні документи: накази, службові записки, інструкції.

2.1.7 Вимоги до патентної чистоти

В комп’ютерній системі повинні використовуватися елементи та

пристрої, програмне забезпечення ліцензовані та сертифіковані для використання на території України.

2.1.8 Вимоги до стандартизації й уніфікації

Система повинна відповідати стандартам групи IEEE 802підгрупи 802.3, що є основою сімейства технологій пакетної передачі данних Ethernet. Необхідно забезпечити уніфікацію даних в системі з міжнародними стандартами: ONVIF (OpenNetworkVideoInterfaceForum), PSIA (PhysicalSecurityInteroperabilityAlliance) CAP (CommonAlertingProtocol)**.**

2.2 Вимоги до видів забезпечення.

2.2.1 Інформаційне забезпечення системи

Склад, структура і способи організації даних у системі.

Робота системи повинна відповідати стандартам провідних компаній розробників Cognimatics (Швеція), Flonomics (США), Aimetis (Канада) потік з одної IP-камери по протоколам ONVIF с роздільною здатністю Full-HD (1920×1080), базовим кодеком H.264 и частотою 25 кадрів в секунду, при умові високої активності вкадріне повинен генерувати трафік більший ніж 7 Мбіт/с.

Організація сховища потрібного обєму при умові використання RAID-7.3 або RAIDN+M.

Підтримка підключення по всіх интерфейсах для блочного і файлового доступу: SAN (FibreChannel, iSCSI, SAS, InfiniBand) і NAS (NFS, AFP, SMB та ін.).

Інформаційний обмін між компонентами системи;

Відповідно до стандарту IEEE 802.3a, обмін між компонентами мережі має використовувати PHY - LAN PHY і WAN PHY.

Інформаційна сумісність із суміжними системами;

Виконання міжнародних стандартів управлінського обліку – MRPII, ERP, CSRP;

2.2.2 Технічне забезпечення системи

Технічні засоби для використання в системі;

В якості центрального комутатора (ядра мережі) використовувати керований комутатор 3-го рівня що підтримує мережеві технології і стандартииDHCP, PORTFORWARDING, VPN,PoweroverEthernet (PoE). Підтримка протоколів IEEE 802.3u, 802.3ab, 802.3z, 802.3x, 802.1D, 802.1w, 802.

Технічні вимоги до відео сервера.

Не менше 128-каналів

Пропускна здатність: вхідна — 400 Мбіт/с, запису — 320 Мбіт/с, вихідна — 96 Мбіт/с.

Підтримка кодеків SmartH.265+, SmartH.264+, H.265, H.264.

Підтримка алгоритмів глибокого навчання.

2.2.3 Вимоги до організаційного забезпечення

Гарантоване розмежування доступу користувачів до програмної та технологічної інформації, які мають містити розмежування доступу по робочих місцях;реєстрація входу (виходу) користувачів в систему,виявлення, ідентифікація і видалення комп'ютерних вірусів.

Доступ до інформації функціональних підрозділів повинен формуватися на основі матриці доступу і повинен дозволяти коригування в процесі експлуатації мережі. Для захисту від помилкових дій персоналу необхідно реалізувати ступінь доступу кожного суб’єкта до інформації Ч – читання; З – зберігання; Д – друкування; К – копіювання; М – модифікація.

2.2.4 Вимоги до складу нормативно-технічної документації системи

До складу повинні входити: робочі креслення, які розробляються згідно з вимогами нормативних– документів (траси прокладання кабелів по

кожній підсистеми, тощо); позначення і правила маркування розеток, кабелів тощо; ескіз монтажу кабелів у різних роз'ємах; схема підключення кабельної проводки; таблиця кабельних з'єднань; плани розміщення обладнання в шафах або стійках; програма і методика випробування.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

3.1Організаційна структура підприємства

Організаційна структура підприємства визначається функціональними підрозділами які є на підприємстві і зв'язками між ними. Структура підприємства відноситься до класу лінійно-функціональних.

Лінійну ланку складають:

директор;

заступник директора;

– каса;

–фінансово-економічна служба;

–служба головного бухгалтера;

– комерційний відділ;

– складські приміщення;

Функціональні ланки:

служба системного адміністратора;

служба охорони;

логістичний відділ.

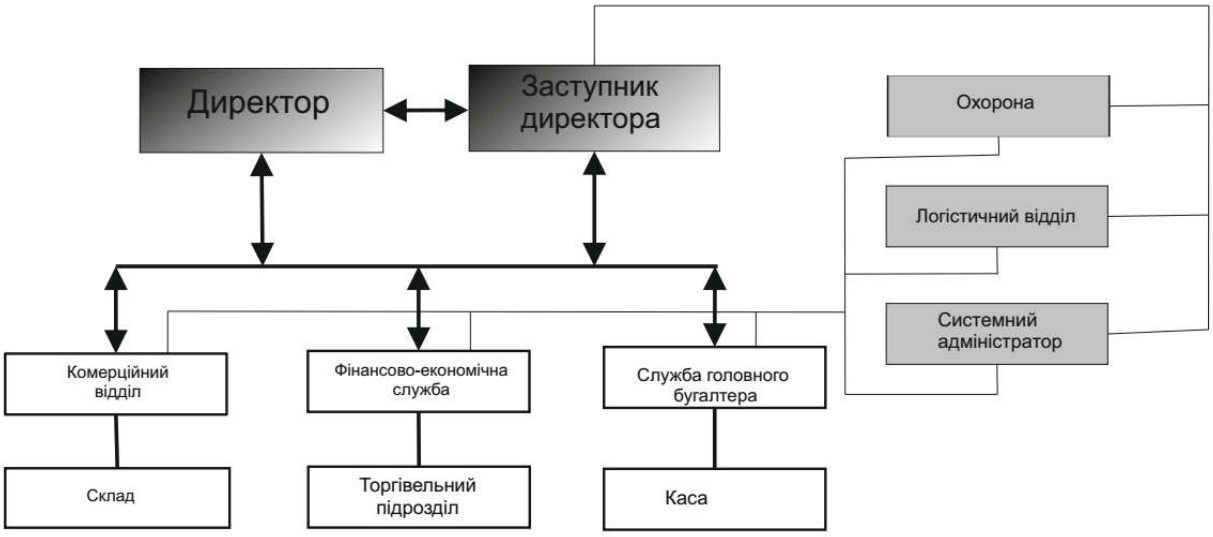

Рисунок 3.1 – Організаційна структура підприємства

Організаційна структура підприємства відноситься до класичної структури. Для ефективної роботи лінійні ланки відносяться до основних «виробничих потужностей», а функціональні – повинні забезпечувати якісне функціонування основної структури.

Доступ до інформаційних ресурсів підприємства розмежований. Відповідно до класу інформаційних ресурсів повнота доступу забезпечується системою паролів.

Враховуючи, що комп'ютерна мережа є розподіленою. До комп'ютерної системи входить мережа відео нагляду [19].

3.2Структура комплексу технічних засобів комп'ютерної мережі підприємства

До структури комплексу технічних засобів комп'ютерної системи підприємства входять: система відео нагляду першого поверху; система відео нагляду другого поверху; комп'ютерна мережа розрахунково-касового обслуговування першого поверху; комп'ютерна мережа офісу другого поверху. Технічні засоби компютерної системи детально показані на декількох рисунках [16,17].

Рисунок 3.2 показує організацію розрахунково касової мережі. Мережа підключена до маршрутизатора другого поверху.

На рисунку 3.2 показане розташування основних елементів комп'ютерної системи першого поверху. До них відноситься розрахунковий касовий вузол, система відеокамер, кімната охорони, у якій ведеться спостереження за ситуацією та розташовані комп'ютери спостереження.

На другому поверсі підприємства розташовані основні вузли комп'ютерної системи. Рисунок 3.4 показує розташування камер відео контролю і відео сервера.

На рисунку 3.5 наведена практично структура головної під мережі підприємства з периферійним обладнанням.

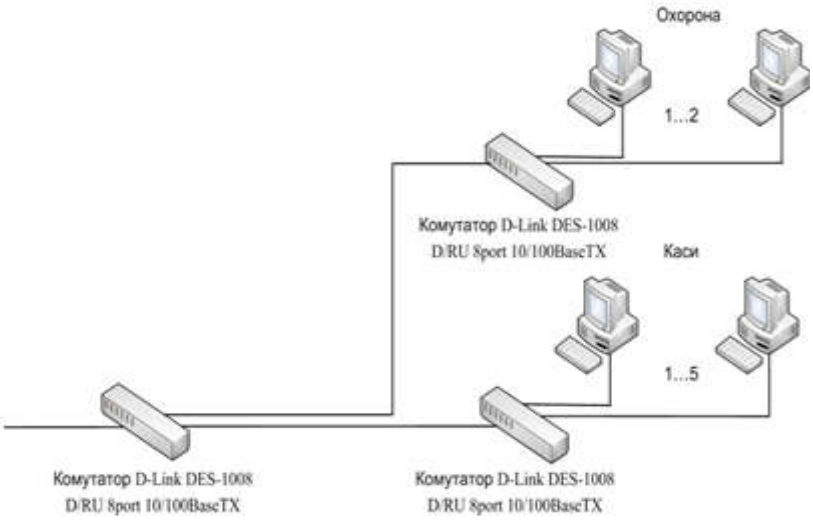

Рисунок 3.2 – Локальна мрежа рорахунково-касового обслуговування

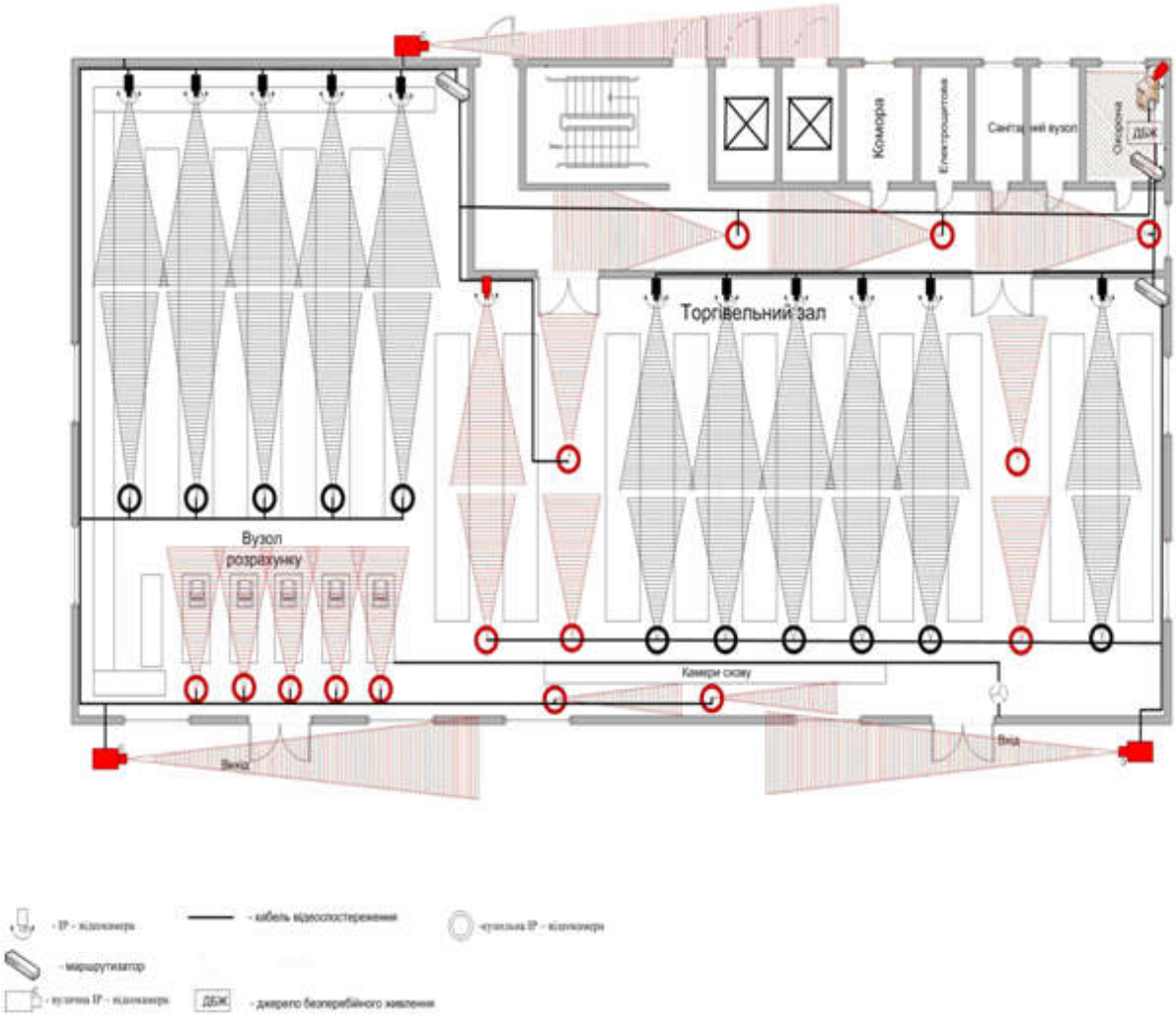

Рисунок 3.3 – Система відео контролю першого повурху

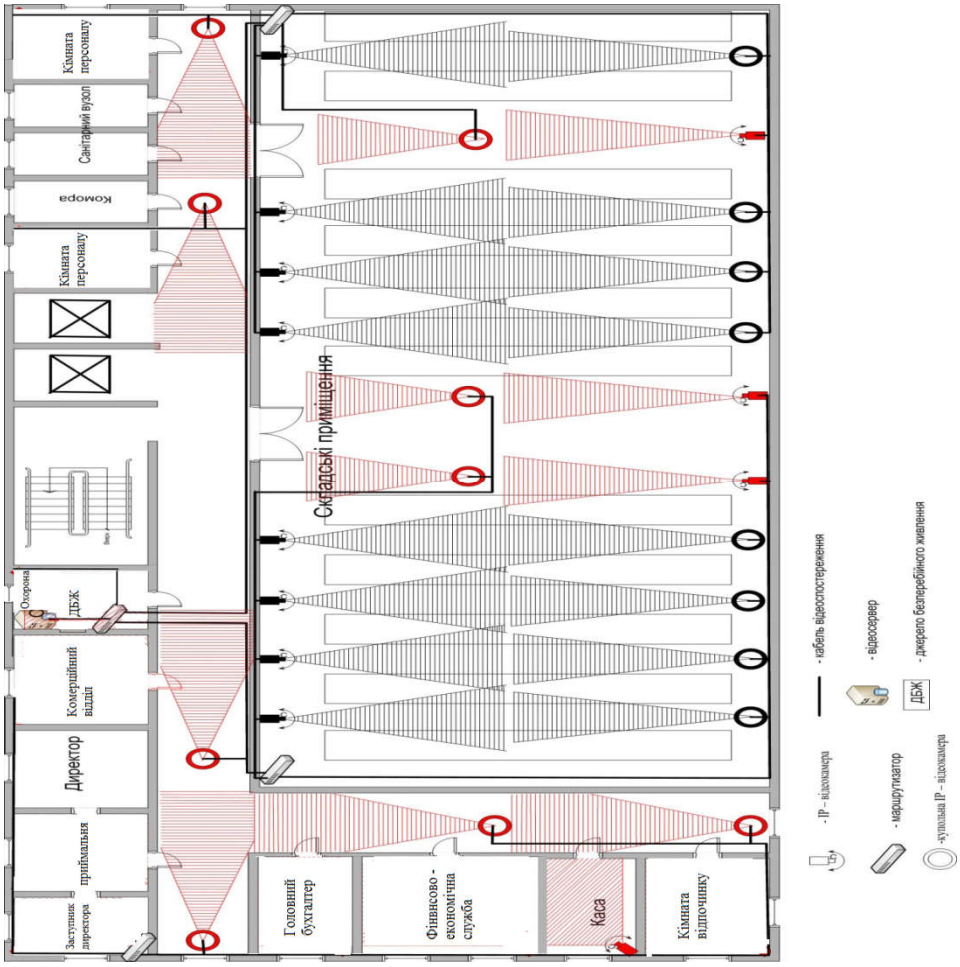

Рисунок 3.4 – Система відео контролю другого поверху

Відеосервер усієї системи відео спостереження встановлено у кімнаті начальника охорони підприємства.Структура системи забезпечення виробничих потреб підприємства стала і в межах потреб повністю задовольняє підприємство.

Система відео нагляду потребує модернізації. На схемах розташування IP – камер червоним кольором виділені камери, які встановлені додатково. А також було виконано роботи по заміні обладнання на більш сучасне.

Зважаючи на існуюче обладнання необхідно провести модернізацію усієї системи підприємства. Заміна комутаторів і маршрутизаторів необхідна у зв’язку із необхідністю підвищення продуктивності комп’ютерних мереж.

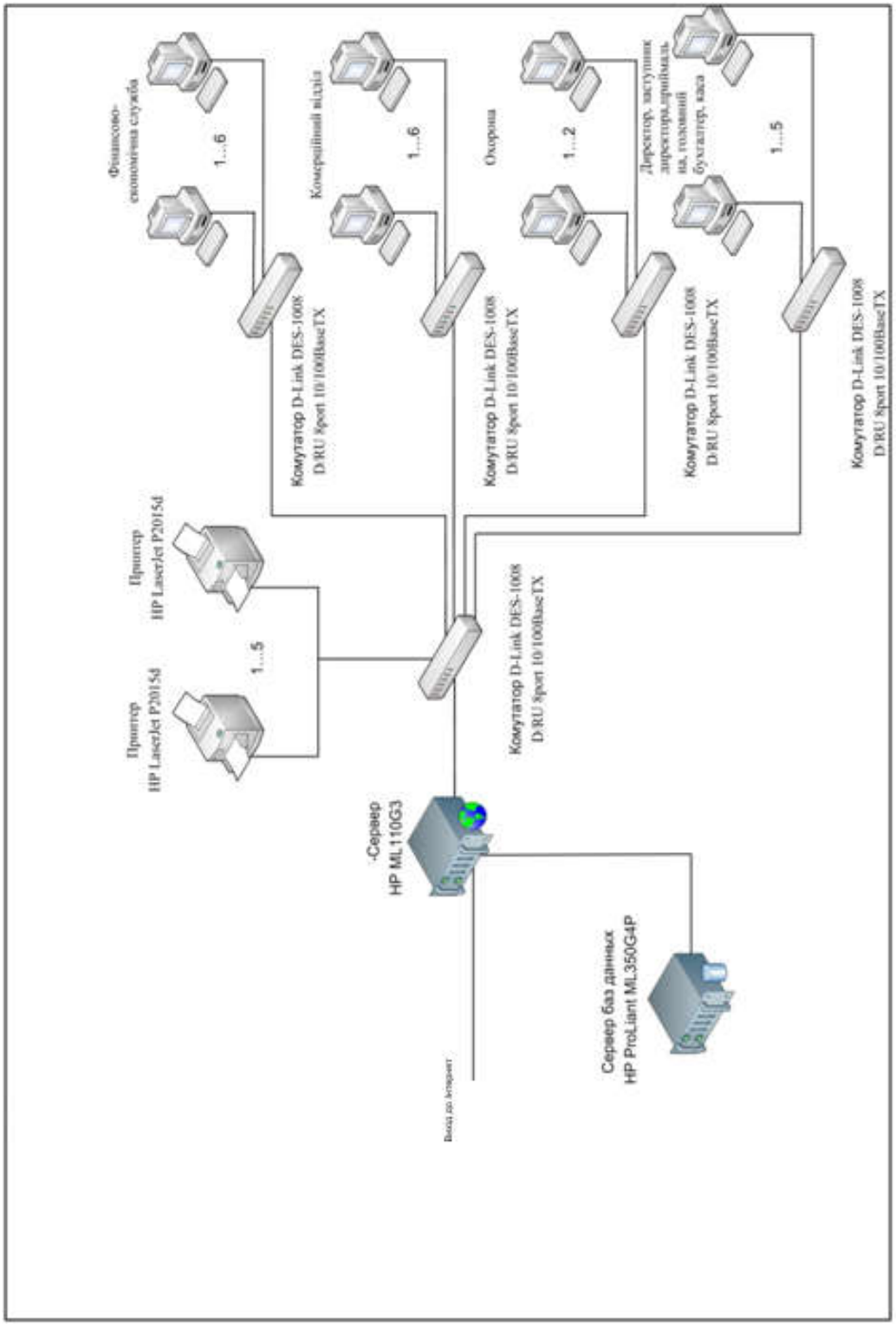

Рисунок 3.5 – Обладнання комп’ютерної мережі другого поверху

3.3 Розробка структурної схеми комп'ютерної системи

Відповідно до характеристик підприємства розроблено структурну схему комп'ютерної мережі підприємства.

На структурній схемі (Рис. 3.6) зображено компютерну мережу яка складається з чотирьох локальних мереж.

LAN1 – локальна мережа, яка об'єднує камери відео спостереження та монітори у кімнаті охорони першого поверху. В торгівельному залі і зовні будівлі розташовано 41 IP камеру. Усі камери отримують живлення від комутатора, комутатор обладнаний відповідним інтерфейсом. Комутатор підключено до маршрутизатора. До цього ж маршрутизатора підключено два термінали відеоспостенреження.

LAN2 – локальна мережа, яка об'єднує камери відео спостереження, монітори відеосервер у кімнаті охорони другого поверху. На другому поверсі розташовано 24 IP камери. Їх підключення до комутатора аналогічне підключенню камер першого поверху. Маршрутизатор LAN2 є центральним для двох локальних мереж і повязує локальні мережі відео спостереження з центральним маршрутизатором усієї системи.

LAN3 iLAN4 – локальні мережі що забезпечують функціонування основних підрозділів підприємства.

LAN3 – об'єднує 8 терміналів. До комутатора підключені термінали комерційного відділу і фінансової служби. Далі через маршрутизатор забезпечується доступ з усією мережею.

LAN4 – об'єднує термінали директора, заступника директора, приймальної, бухгалтерії, каси і п'яти касових терміналів торгівельної зали.

Усі локальні мережі підключені до одного маршрутизатора, до якого також підключений комутатор термінала системного адміністратора і центрального сервера.

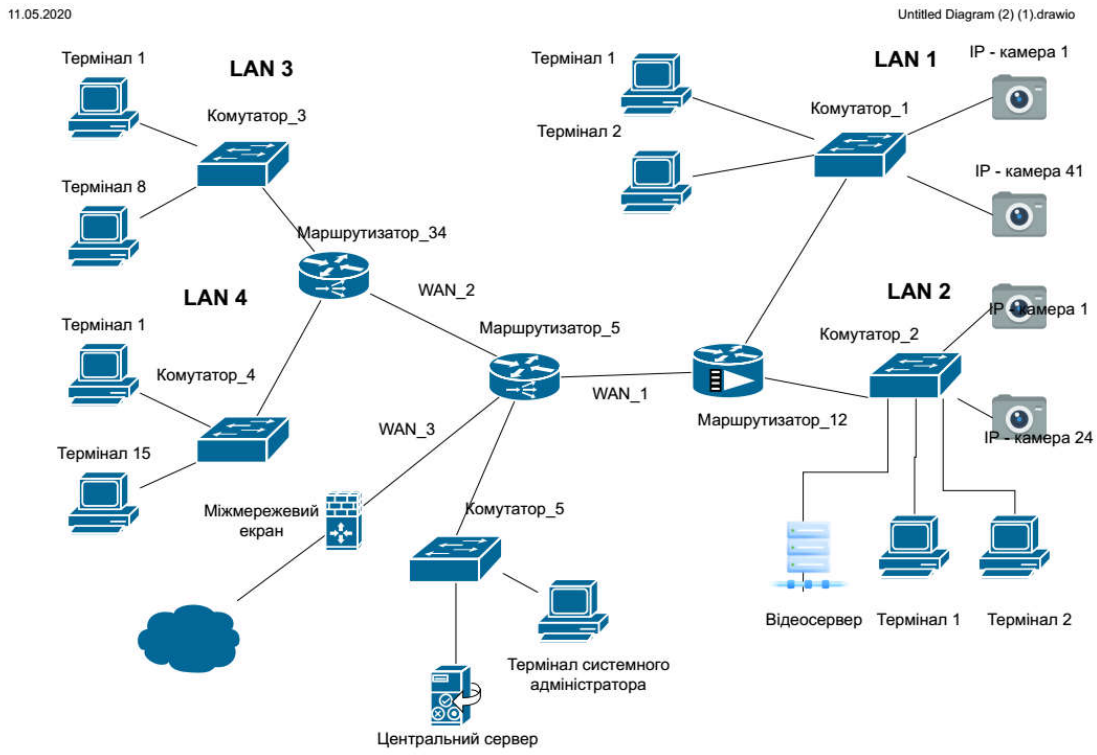

Рисунок 3.6 – Структура комп’ютерної мережі підприємства

3.4 Вибір та характеристики апаратних засобів комп’ютерної мережі

Характеристики використовуваних комутаторів.

Локальна мережа 1 використовує спеціалізований комутатор на 48 входів для відеокамер.

Комутатор L2 GigabitEthernetPoED-linkDGS-3120-48PC

Цей комутатор оснащений 50 LAN-портами, які діляться на три типи: 44 гігабітних порту Base-T, 4 комбінованих гігабітних порту Base-T / SFP і 2 10-гігабітних uplink-портівCX4. Оснащений додатковим джерелом живлення DPS-700, консольним портом з роз'ємом RJ-45, який так само є засобом управління, 2 порти для роботи в стеку і 1 слот для карти пам'яті SD. Пропускна здатність даного пристрою становить 136 Гбіт в секунду завдяки технології комутаційної матриці. Обсяг передачі даних досягає 101.19 мільйона пакетів в секунду. LAN-порти так само підтримують технологію PoE зі стандартами 802.3af / at. Має можливості роботи як в фізичному стеці

комутаторів, так і у віртуальному з 6 або 32 пристроями в залежності від того, який з вищевказаних типів стекування використовується. Підтримує безліч функцій, засоби для проведення віртуальних локальних мереж, а так же функціонал QoS для контролю та оптимізації смуги пропускання. Має великий набір функцій для управління та забезпечення безпеки.

Інтерфейси 44 10/100/1000BASE-T, 4 комбо-порта 10/100/1000BASE-T/SFP, 2 10GCX4

Резервнеджерело живлення DPS-700

Консольний портRJ-45

Додаткові слоти 2 порта для стекування, 1 Слот для SD-картки

ПотужністьКомутаційнна матриця 136 Гбит/с, Швидкість перенаправлення 64-байтних пакетів 101,19 Mpps, буфер пакетів 2 Мб, Flash-память 32 Мб

Стандарт PoE802.3af, 802.3at

ПотужністьPoE370 Вт, 740 Вт (зDPS-700 RPS)

Можливості комутатора стекування (фізичне/віртуальне), функциії рівня 2/3, багато адресне розсилання рівня 2, маршрутизація рівня 3, VLAN, якість обслуговування (QoS), списки управління доступом (ACL), AAA, D-LinkGreen, OAM, DDM, стандартиMIB/RFC, EAP.

MTBF (Часи)223006

Рівень шуму Макс 48.6 db, Мін 41.6 db

Тепловиділення 1761,265 BTU/ч (370 Вт для PoE), 3310,428 BTU/ч (740Вт для PoE)

Живлення на вході 100-240 В, внутрішнє універсальнеджерело живлення з PFC

Макс. Потужність 516,5 Вт (370 Вт для PoE), 970,8 Вт (740 Вт для PoE)

Локальна мережа 2 використовує спеціалізований комутатор на 24 входи для відеокамер.

Комутатор L2 Gigabit Ethernet PoE Planet GS-4210-24P4C

Світч GS-4210-24P4C є продуктивним і надійним рішенням від Planet, необхідно організувати корпоративну або інших типів середню / велику мережу з керуванням рівня L2. Оснащено пристрій 24 інтерфейсами класу Gigiabit E, на кожному з яких підтримується Poe, а також чотирма комбінованими з SFP портами. Комутатор має матрицю зі швидкістю комутації близько 56 Gbps. Дана модель GS-4210-24P4C пропонує адміністраторам мереж вичерпний набір функцій, включаючи підтримку IPv6 протоколів, QoS, VLAN, а також управління трафіком, портами, доступом, підвищену безпеку і багато іншого. Переваги світча GS-4210-24P4C - це висока продуктивність в сумі з доступністю і надійністю.

Порти Ethernet28x 10/100/1000BASE-T RJ45 Auto-MDI/MDI-X

SFP/mini-GBIC слоти 4x 100/1000BASE-X SFP об'єднані зпортами 25-28, підтримка 100/1000Mbps dual mode и DDM

PoE порти 24x порти 802.3at/af PoE порти 1-24

Консольний порт1x RS232 (RJ45) (115200, 8, N, 1)

ТипкомутатораStore-and-Forward

Швидкістьпередачіданих56Gbps / non-blocking

Буфер4.1 Мб

УправлінняпотокомIEEE 802.3x pause frame for full-duplex, Back pressure for half-duplex

Індикатори PWR, SYS, LNK/ACT, PoE-in-Use, 1000, FAN 1 Alert, FAN 2 Alert, PoE PWR Alert

Живлення100~240 В AC, 50/60Hz

Габарити 440 x 300 x 44.5 мм, 1U

Захист від статичного разряду 2 кВ DC

Споживанапотужність275 Вт / 938.3 BTU

PoEстандарти IEEE 802.3af / 802.3atPoE+ PSE

PoE потужність 220 Вт @ 25 C, 190 Вт @ 50 C

VLAN802.1Q tagged-based VLAN, до 256 VLAN груп, 4094 VLAN IDs, 802.1ad Q-in-Q tunneling, Voice VLAN, Protocol VLAN, Private VLAN GVRP

Протоколи STP, IEEE 802.1D Spanning Tree Protocol, RSTP, IEEE 802.1w Rapid Spanning Tree Protocol, MSTP, IEEE 802.1s Multiple Spanning Tree Protocol

Управління Веб-браузер / Telnet / SNMP v1, v2c, оновлення HTTP / TFTP через Ethernet, віддалений / локальнийжурнал, системнийжурнал, LLDP протокол, SNTP

Локальна мережа 3 використовує комутатор на 8 входів.

Комутатор L3 Gigabit Ethernet Cisco SG300-20

Комутатор відноситься до серії пристроїв для забезпечення комунікаційної життєдіяльності офісу малого і середнього бізнесу. Він оснащений сучасними протоколами зв'язку для більшої надійності внутрішньокорпоративної мережі. Одночасне використання пристроїв, що підключаються можливо без ризику збоїв і вильоту з системи завдяки даним системам безпеки. Комутатор представляє собою сучасне високопродуктивний пристрій для роботи техніки на високих швидкостях передачі цифрових даних. Крім того, комутатор оснащений гігабітними портами нового покоління для підключення сучасних пристроїв. Всього підтримує велику кількість інтерфейсів для великого числа підключень високопродуктивних функціональних пристроїв, що забезпечують надійну роботу вашої корпоративної системи зв'язку.

Технологія доступу Ethernet

Тип розємівRJ-45, SFP

Тип кабелю Вита пара

КількістьLAN портів8 шт

Тип LAN портівSFP

Кількістьuplink-портів2 шт

Тип uplink-портів10/100/1000 Base-TX (1000 мбит/с) ComboSFP

Протоколи Ethernet IEEE 802.3a, IEEE 802.3ab, IEEE 802.3u, Web-інтерфейс.

Локальна мережа 3 використовує комутатор на 24 входи.

Комутатор L3 Fast Ethernet Cisco SF500-24-K9-G5

Комутатор простий в управлінні і дозволяє вирішити більшу кількість завдань при невеликій вартості самого пристрою,з широким набором функцій і продуктивністю комутатора. Кращий засіб для організації комутаційної системи для підприємств малого та середнього бізнесу. Дозволяє побудувати безпечну, надійну високопродуктивну зв'язок всередині офісу. Вбудовані сучасні протоколи зв'язку допомагають реалізувати весь потенціал для безперебійної та високопродуктивної системи комунікації. Додаткові функції дозволять вирішити більшу кількість завдань і оптимізують бізнес-процеси для вашої зручності.

Порти Fast Ethernet 24 шт, Gigabit Ethernet 2 шт, SFP (оптика) 4 шт

Функції Управління SSH, Telnet

Web-інтерфейсSNMP

Базовіможливості **DHCP**Підтримкастекування, VLAN, захиствідпетель

В мережі використані гігабітні роутери. В локальних мережах 1 і 2 використані роутери з відповідною кількістю входів.

Роутер Cisco RV345P-K9-G5

Рисунок 3.7 – Вигляд роутера моделі RV345P-K9-G5

Модель RV345P-K9-G5 серії SmallBuisness виробництва компанії Cisco є компактним, але продуктивною VPN-роутером для невеликих мереж малого бізнесу. Оснащений двома WAN-портами, а також 16 портами LAN номіналом 1Gbps. Крім цього, є також два USB-роз'єми для підключення 3G / 4G модемів. Дана модель передбачає розширений VPN-функціонал.

Порти кількість WAN портов 2 x 10/100/1000TX, количество LAN портов 16 x 10/100TX/1000TX, USB x 2, дополнительные порты и разъемы: USB /3G/4G Dongle

Безпровідна мережа захист інформації, брандмауэр IPv6.

Пропускна здатність IPsec VPN (DES): 650 Мбит/с

Мережеве управління, віддалене управління: SNMP /1, 2c, 3, HTTPS, HTTP.

Провідна мережа

- підтримка транспортних протоколів: PPPoE, TCP/IP, DHCP, IPsec, PPTP, L2TP, UDP/IP.
- стандарти: IEEE 802.3x, IEEE 802.1X, IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1p, IEEE 802.3af, IEEE 802.3az, FCCClassAcertified, UL, BSMI, cUL, CB, CCC, ANATEL, KC.
- функції міжмережевогоекрану: NAT, PAT.
- протоколы: RIP /1, 2, ng, IGMP,IPv6, Static IP, ALG, DHCP client, GRE.

Додатково підтримка SIP, QoS.

Роутер Cisco RV320-K9-G5

Рисунок 3.8 – Вигляд роутера моделі RV320-K9-G5

Модель RV320-K9-G5 виробництва компанії Cisco є VPN-роутер для домашніх або ж невеликих офісних мереж. Підтримує стандарт бездротового зв'язку 802.11n і працює на частоті 2.4 ГГц. В наявності один WAN-порт номіналом 1 Гбіт / с, один DMZ-портом, а також чотири LAN і один USB-роз'єм. Дана модель передбачає розширений VPN-функціонал.

Стандарт WiFi

- 802.11 b/g/n

Частота

- 2,4 ГГц

Інтерфейси

- 4x10/100/1000 Gigabit Ethernet LAN
- 1x10/100/1000 Gigabit Ethernet WAN
- 1x10/100/1000 Gigabit Ethernet DMZ
- 1xUSB (3G/4G USB Failover)

VPN

- 25x IPsec, 10x SSL VPN, 10x PPTP

Додаткові функції

- IPSec, SSL, L2TP VPN
- NAT, PAT

Міжмережевий екран ZyXELZyWALLUSG 40 (USG40-RU0101F)

Швидкість WAN 1 Гбит/с

Кіл-тьRJ-45 LAN 1Гбит/с 3 шт.

Інші розєми 1xRJ-45 WAN, RJ-45 (консольний)

ПротоколыSIP/H.323, FTP, IPSec, L2TP, PPTP, MSN и RTP, IPv6

Підтримка USB 3G/4G-модемаHuawei: E3276s-150, E3272s-153, E3272 (M100-4); Novatel:USB551L; Pantec: UML290; Yota: WLTUBA-107; ZTE: MF823, MF823

Пам’ять 4 МБ (оперативна пам’ять), 4 МБ (вбудована).

IP-відеокамера

Рисунок 3.9 – Вигляд IP-відеокамери HIKVISION

Основні характеристики

Запис на SD карту пам'яті, на жорсткий диск HDD, в хмару

Вид циліндрична

Дальність ІЧ-підсвічування30 метрів

Особливості. Віддалений перегляд, ІК підсвічування, відеоаналітіка, розпізнавання осіб, висока роздільна здатність 4мп.

Тип підключення. Провідні, PoE.

Вулична, Внутрішня

Об'єктив4 мм

Клас захистуIP67, TVS 2000

Матриця1/3 "Progressive Scan CMOS

СпоживанняDC 12В ± 25% / 6 Вт, PoE (802.3af)

Кут огляду78

Чутливість0.01 Люкс / (F1.2, AGC вкл), 0.018 Люкс / (F1.6, AGC вкл); 0 Люкс з ІК

Сервер DellEMCPowerEdge

T140 дозволяє виконувати типові робочі навантаження сучасного бізнесу за доступною ціною.

Ідеально підходить для наступних бізнес-додатків:

• Зберігання файлів і друк

• Робота з електронною поштою та системою передачі повідомлень

•Платіжний термінал

• Фінанси

• Підвищення ефективності роботи за рахунок збільшення на 50% кількості ядер процесора Intel Xeon E-2100, підвищення швидкостей передачі даних на 11% і збільшення кількості каналів PCIe на 20%

• Підвищення швидкодії на 66% за допомогою набору послуг ProDeploy

• Вирішення проблем і скорочення до 72% трудомісткості операцій IT за допомогою автоматизованої технології профілактики та прогнозів на базі ProSupport Plus і SupportAssist

• Надає можливість застосування гнучких варіантів розміщення в корпусах tower з низьким рівнем шуму і високою ефективністю охолодження

Тип процессораIntelXeonE-2124 3.3GHz, 8Mcache, 4C/4T, turbo (71W)

КількістьGigabitEthernet – 3шт.

РейдконтролерPERCH330.

Обладнання мережі обрано з розрахунку на те щоб забезпечити гігабітні швидкості обміну інформацією як всередині мережі так і з мережею інтернет.

3.5 Захист інформації в комп'ютерній системі

На даному підприємстві у зв'язку з його діяльністю циркулює відкрита та конфіденційна інформація.

До відкритої інформації підприємства відноситься:

– інформація про діяльність фірми;

– інформація про товари та послуги.

До конфіденційної інформації підприємства відноситься:

– інформація про плани підприємства;

– інформація про фінанси підприємства;

– договори про надання клієнтам послуг;

– інформація про партнерів підприємства;

– персональні дані співробітників;

– трудові договори співробітників;

– внутрішні документи: накази, службові записки, інструкції.

3.5.1 Загрози інформаційної безпеки

Всі джерела загроз безпеці інформації можна розділити на три основні групи [15]:

I. Обумовлені діями суб'єкта (антропогенні джерела загроз).

II. Обумовлені технічними засобами (техногенні джерела загрози).

III. Обумовлені стихійними джерелами.

Антропогенним джерелом загроз є суб'єкт, що має санкціонований або несанкціонований доступ до роботи зі штатними засобами підприємства. Суб'єкти, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні, так і внутрішні.

До зовнішніх антропогенних джерел загроз належать:

– кримінальні структури;

– потенційні злочинці та хакери;

– несумлінні партнери;

– технічний персонал постачальників телематичних послуг;

– представники наглядових організацій і аварійних служб;

– представники силових структур.

До внутрішніх антропогенних джерел загроз належать:

– основний персонал (користувачі, програмісти, розробники);

– представники служби захисту інформації;

– допоміжний персонал (прибиральники, охорона);

– технічний персонал (життєзабезпечення, експлуатація).

Техногенні джерела загроз напряму залежать від властивостей техніки. Технічні засоби, що є джерелами потенційних загроз безпеки інформації також можуть бути зовнішніми і внутрішніми.

3.5.2 Доступ до інформації з відеоконтролю

За системою відеоспостереження слідкують охоронники, які знаходяться в кабінеті охорони на першому та другому поверсі. В їх обов‘язки входить забезпечення безперебійної роботи системи відеоспостереження, контроль за дотриманням правил доступу до відеоданих та робота з відеоінформацією.

Таким чином, доступ до відеоінформації відкрито таким співробітникам:

– директор;

– заступник директора;

– охоронці.

При цьому перелічені співробітники матимуть наступні права доступу до відеоінформації:

– директор – перегляд, зберігання, знищення, копіювання, модифікація;

– заступник директора – перегляд;

– охоронці – перегляд.

Усі інші співробітники доступ до відеоінформації не мають.

Таким чином на підприємстві «Вітязь» було вдосконалено систему відеоспостереження, зменшено кількість мертвих зон, розмежований доступ до відеоінформації.

3.5.3 Методи та засоби захисту відеопотоку даних

Технологія DRM – Digital Rights Management, яка в даний час актуальна в сфері захисту авторських прав для цифрових продуктів також призначена для забезпечення збереження відеопотоку, що передається й запобігання неавторизованому доступу до нього. Цифрові права доступу – це правила, що визначають те, що конкретним користувачам, які працюють з відповідною інформацією, дозволено робити з нею.

На даний час технологія має широке вживання серед компаній та виробників, бажаючих зберегти авторське право, наприклад, на музичний твір або на будь який відеоматеріал, а також бажаючих запобігти несанкціонованому копіюванню мультимедіа інформації. Звісно, що використання цієї технології не може бути обмежене лише комерційною метою. DRM може бути важливим елементом захисту інформації на підприємстві. Наприклад, якщо технологія буде використовуватися для удосконалення системи відеоспостереження організації. Тому що за останні роки відеоспостереження стало невід'ємною частиною комплексної системи безпеки об'єкта, оскільки сучасні системи дозволяють не тільки спостерігати й записувати відео, але й програмувати реакцію всієї системи безпеки при виникненні тривожних подій або ситуацій [14].

Технологія, що одержала назву FairPlay (англ. – чесна гра), в 2001 році була ліцензована компанією Apple Computers.

FairPlay використовує метод кодування. В її роботі беруть участь:

– сервер ITunes;

– контент в аудіоформаті AAC (Advanced Audio Coding), закодований з використанням алгоритмів FairPlay;

– програма ITunes, встановлена на ПК покупця;

– плеєр Ipod.

При необхідності накладення на інформацію обмеження доступу програмою ITunes, сервер кодує дані за допомогою ключа Master Key. Потім даний ключ у свою чергу кодується ключем, іменованим User key (ключ користувача). MP4-контейнер, який отримує користувач, містить закодований файл і закодований майстер-ключ. Окремо, після підтвердження з'єднання, висилається ключ користувача. Ключ користувача індивідуальний для кожного потоку даних.

Програма ITunes, встановлена на ПК користувача, зберігає всі ключі користувача в спеціальній базі даних. База даних у свою чергу закодована ще одним ключем, іменованим System key (ключ системи), індивідуальним для

кожного комп'ютера. Друга копія бази даних ключів користувача зберігається на сервері ITunes в профілі користувача. Там же зберігаються і ключі системи.

Ця система дозволяє реалізувати всі можливості і обмеження FairPlay DRM. При програванні захищеного файлу з комп'ютера ITunes декодує відповідний User key, використовуючи індивідуальний System key ПК. Відповідно, ITunes, встановлений на „чужій" машині, програти цей файл не буде здатна, тому що не володіє вірним User key.

Така трьохступенева система позбавляє користувача прямого доступу до декодера майстер-ключа, а також прив'язує цей ключ до конкретного комп'ютера, що, власне, і є головним завданням DRM.

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

Сертифікат – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача [7];

Зазвичай підписуємі файли мають змінну (і досить велику) довжину, в схемах ЕЦП найчастіше підпис ставиться не на сам документ (дані), а на його хеш. Для обчислення хеша використовуються криптографічні хеш-функції, що гарантує виявлення змін документа при перевірці підпису. Хеш-функції не є частиною алгоритму ЕЦП, тому в схемі може бути використана будь-яка надійна хеш-функція.

Алгоритми ЕЦП поділяються на два великих класи: звичайні цифрові підписи та цифрові підписи з відновленням документа. Звичайні цифрові підписи необхідно додавати до підписуємих документів. Цифрові підписи з відновленням документа містять в собі підписуваємий документ: в процесі перевірки підпису автоматично обчислюється і тіло документа.

Завдання захисту ключів від підміни вирішується за допомогою сертифікатів. Сертифікат дозволяє посвідчити укладені в ньому дані про власника і його відкритий ключ підписом якої-небудь довіреної особи. У централізованих системах сертифікатів (наприклад PKI) використовуються центри сертифікації, підтримувані довіреними організаціями. У децентралізованих системах (наприклад PGP) шляхом перехресного підписання сертифікатів знайомих і довірених людей кожним користувачем будується мережа довіри [7].

4. ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

4.1 Розрахунок адресації комп'ютерної мережі та схеми адресації пристроїв

В кваліфікаційній роботі необхідно змоделювати комп'ютерну мережу згідно заданої структури (рисунок 3.6) в PacketTracer за наступними вимогами з адресації: адреса для виділення підмереж: 192.168.88.0/21

Кількість вузлів приведена в таблиці 4.1. Налаштування паролів базової конфігурації пристроїв приведене у таблиці 4.2.

Таблиця 4.1 – Кількість вузлів у підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
44	28	9	16	3

LAN1 – мережа «1поверх «Торгівельна зала»»

LAN2 – мережа «Другий поверх»

LAN3 – Мережа «Менеджмент»

LAN4 – Мережа «Касово розрахункова та фінансові служби»

LAN5 – Мережа «Системний адміністратор»

Таблиця 4.2 – Налаштування паролів базової конфігурації пристроїв

Паролі		
консолі і vty	привілейованого режиму	користувача
cisco12317sk	*class12317sk*	*Prihodko*

На рисунку 3.6 приведено структуру комп'ютерної мережі, яка повинна бути розроблена у роботі. На основі цієї структури була розроблена модель комп'ютерної мережі. Схема моделі приведена на рисунку 4.1.

На рисунку 3.6 приведено структуру комп'ютерної мережі, яка повинна бути розроблена у роботі. На основі цієї структури була розроблена модель комп'ютерної мережі.

Організації виділено один блок IP-адрес 192.168.88.0/21, який треба розбити на 5 різних за розмірами підмереж (LAN1– 43, LAN2 – 27, LAN3 – 9, LAN4 – 16 LAN5 – 3). Слід врахувати, що кожна пара маршрутизаторів також з'єднується між собою окремою підмережею, тому буде потрібно ще 4 невеликих підмережі. Оскільки такі підмережі містять тільки по два хоста, для них достатньо використовувати префікс підмережі /30.

Так як розміри підмереж різні, то для розрахунку адресації мереж використовуватимемо метод VLSM (Variable Length Subnet Masks, RFC 950). При використанні VLSM мережа поділяється на підмережі, а потім кожна підмережа розділяється знову. Цей процес може повторюватися кілька разів і дозволяє створювати підмережі різних розмірів, виходячи з необхідної кількості вузлів для кожної підмережі.

Виділений блок 192.168.88.0/21 дає можливість адресувати $2^{32-21}-2=2^{11}-2=2046$ пристроїв. Для потреб організації потрібно 100 адрес, таким чином тільки 70% адресного простору використано.

Для мережі LAN1 на 12 вузлів:

маска 255.255.255.192 (або префікс /26). Діапазон адрес 192.168.88.1 - 192.168.88.62. Широкомовлення 192.168.88.63. Для адресації 44 пристроїв використовуемо адреси 192.168.88.20 - 192.168.88.62. Блок адрес 192.168.88.2 - 192.168.88.19 залишається вільним.

Мережа LAN2, маска 255.255.255.224 (або префікс /27). Діапазон адрес 192.168.88.65 - 192.168.88.94. Широкомовлення 192.168.88.95. Для адресації 28 пристроїв використовуемо адреси 192.168.88.68 - 192.168.88.94. Блок адрес 192.168.88.66 - 192.168.88.67 залишається вільним.

Для мережі LAN3 на 9 вузлів:

маска 255.255.255.240 (або префікс /28). Діапазон адрес 192.168.88.129 - 192.168.88.142. Широкомовлення 192.168.88.143. Для адресації 9 пристроїв

використовуємо адреси 192.168.88.134 - 192.168.88.142. Блок адрес 192.168.88.130 - 192.168.88.133 залишається вільним.

Для мережі LAN4 на 16 вузлів:

маска 255.255.255.224 (або префікс /27). Діапазон адрес 192.168.88.97 - 192.168.88.126. Широкомовлення 192.168.88.127. Для адресації 16 пристроїв використовуємо адреси 192.168.88.111 - 192.168.88.126. Блок адрес 192.168.88.98 - 192.168.88.110 залишається вільним.

Для мережі LAN5 на 3 вузли:

маска 255.255.255.248 (або префікс /29). Діапазон адрес 192.168.88.145 - 192.168.88.150. Широкомовлення 192.168.88.151. Для адресації 2 пристроїв використовуємо адреси192.168.88.149, 192.168.88.150.

Виконуємо подібні розрахунки для наступних мереж WAN (табл.4.3).

Таблица 4.3 – Схема адресування мережі

Ім’я мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
LAN1	44	192.168.88.0	255.255.255.192	192.168.88.1	192.168.88.62
LAN2	28	192.168.88.64	255.255.255.224	192.168.88.65	192.168.88.94
LAN3	9	192.168.88.128	255.255.255.240	192.168.88.129	192.168.88.142
LAN4	16	192.168.88.96	255.255.255.224	192.168.88.97	192.168.88.126
LAN5	3	192.168.88.144	255.255.255.248	192.168.8.145	192.168.88.150
WAN1	2	10.0.12.0	255.255.255.252	10.0.12.1	10.0.12.2
WAN2	2	10.0.12.4	255.255.255.252	10.0.12.5	10.0.12.6
WAN3	2	10.0.12.8	255.255.255.252	10.0.12.9	10.0.12.10

В таблиці 4.4 перелічені адреси всіх пристроїв у мережі.

Таблиця 4.4 – Адреси всіх пристроїв у мережі

Им’я пристрою	Інтерфейс	IP адреса	Маска	Шлюз	VLAN	Для ПК інтерфейс підключеного пристрою
Охорона1_LAN1	-	192.168.88.20	255.255.255.192	192.168.88.1		Fa0/2
Охорона2_ LAN1	-	192.168.88.21	255.255.255.192	192.168.88.1		Fa0/3
IP камера 1_ LAN1	-	192.168.88.22	255.255.255.192	192.168.88.1		8001
IP камера 2_ LAN1	-	192.168.88.23	255.255.255.192	192.168.88.1		8002

IP камера 3_ LAN1	-	192.168.88.24	255.255.255.192	192.168.88.1		8003
IP камера 4_ LAN1	-	192.168.88.25	255.255.255.192	192.168.88.1		8004
IP камера 5_ LAN1	-	192.168.88.26	255.255.255.192	192.168.88.1		8005
IP камера 6_ LAN1	-	192.168.88.27	255.255.255.192	192.168.88.1		8006
IP камера 7_ LAN1	-	192.168.88.28	255.255.255.192	192.168.88.1		8007
IP камера 8_ LAN1	-	192.168.88.29	255.255.255.192	192.168.88.1		8008
IP камера 9_ LAN1	-	192.168.88.30	255.255.255.192	192.168.88.1		8009
IP камера 10_ LAN1	-	192.168.88.31	255.255.255.192	192.168.88.1		8010
IP камера 11_ LAN1	-	192.168.88.32	255.255.255.192	192.168.88.1		8011
IP камера 12_ LAN1	-	192.168.88.33	255.255.255.192	192.168.88.1		8012
IP камера 13_ LAN1	-	192.168.88.34	255.255.255.192	192.168.88.1		8013
IP камера 14_ LAN1	-	192.168.88.35	255.255.255.192	192.168.88.1		8014
IP камера 15_ LAN1	-	192.168.88.36	255.255.255.192	192.168.88.1		8015
IP камера 16_ LAN1	-	192.168.88.37	255.255.255.192	192.168.88.1		8016
IP камера 17_ LAN1	-	192.168.88.38	255.255.255.192	192.168.88.1		8017
IP камера 18_ LAN1	-	192.168.88.39	255.255.255.192	192.168.88.1		8018
IP камера 19_ LAN1	-	192.168.88.40	255.255.255.192	192.168.88.1		8019
IP камера 20_ LAN1	-	192.168.88.41	255.255.255.192	192.168.88.1		8020
IP камера 21_ LAN1	-	192.168.88.42	255.255.255.192	192.168.88.1		8021
IP камера 22_ LAN1	-	192.168.88.43	255.255.255.192	192.168.88.1		8022
IP камера 23_ LAN1	-	192.168.88.44	255.255.255.192	192.168.88.1		8023
IP камера 24_ LAN1	-	192.168.88.45	255.255.255.192	192.168.88.1		8024
IP камера 25_ LAN1	-	192.168.88.46	255.255.255.192	192.168.88.1		8025
IP камера 26_ LAN1	-	192.168.88.47	255.255.255.192	192.168.88.1		8026
IP камера 27_ LAN1	-	192.168.88.48	255.255.255.192	192.168.88.1		8027
IP камера 28_ LAN1	-	192.168.88.49	255.255.255.192	192.168.88.1		8028
IP камера 29_ LAN1	-	192.168.88.50	255.255.255.192	192.168.88.1		8029
IP камера 30_ LAN1	-	192.168.88.51	255.255.255.192	192.168.88.1		8030
IP камера 31_ LAN1	-	192.168.88.52	255.255.255.192	192.168.88.1		8031
IP камера 32_ LAN1	-	192.168.88.53	255.255.255.192	192.168.88.1		8032
IP камера 33_ LAN1	-	192.168.88.54	255.255.255.192	192.168.88.1		8033
IP камера 34_ LAN1	-	192.168.88.55	255.255.255.192	192.168.88.1		8034
IP камера 35_ LAN1	-	192.168.88.56	255.255.255.192	192.168.88.1		8035
IP камера 36_ LAN1	-	192.168.88.57	255.255.255.192	192.168.88.1		8036
IP камера 37_ LAN1	-	192.168.88.58	255.255.255.192	192.168.88.1		8037
IP камера 38_ LAN1	-	192.168.88.59	255.255.255.192	192.168.88.1		8038
IP камера 39_ LAN1	-	192.168.88.60	255.255.255.192	192.168.88.1		8039

IP камера 40_ LAN1	-	192.168.88.61	255.255.255.192	192.168.88.1		8040
IP камера 41_ LAN1	-	192.168.88.62	255.255.255.192	192.168.88.1		8041
Керівник охорони 1_ LAN2	-	192.168.88.68	255.255.255.224	192.168.88.65		Fa0/4
Заступник кер. Охор.1_LAN2	-	192.168.88.69	255.255.255.224	192.168.88.65		Fa0/5
Відеосервер_LAN2	-	192.168.88.70	255.255.255.224	192.168.88.65		Fa0/4
IP камера 1_ LAN2	-	192.168.88.71	255.255.255.192	192.168.88.65		8025
IP камера 2_ LAN2	-	192.168.88.72	255.255.255.192	192.168.88.65		8026
IP камера 3_ LAN2	-	192.168.88.73	255.255.255.192	192.168.88.65		8027
IP камера 4_ LAN2	-	192.168.88.74	255.255.255.192	192.168.88.65		8028
IP камера 5_ LAN2	-	192.168.88.75	255.255.255.192	192.168.88.65		8029
IP камера 6_ LAN2	-	192.168.88.76	255.255.255.192	192.168.88.65		8030
IP камера 7_ LAN2	-	192.168.88.77	255.255.255.192	192.168.88.65		8031
IP камера 8_ LAN2	-	192.168.88.78	255.255.255.192	192.168.88.65		8032
IP камера 9_ LAN2	-	192.168.88.79	255.255.255.192	192.168.88.65		8033
IP камера 10_ LAN2	-	192.168.88.80	255.255.255.192	192.168.88.65		8034
IP камера 11_ LAN2	-	192.168.88.81	255.255.255.192	192.168.88.65		8035
IP камера 12_ LAN2	-	192.168.88.82	255.255.255.192	192.168.88.65		8036
IP камера 13_ LAN2	-	192.168.88.83	255.255.255.192	192.168.88.65		8037
IP камера 14_ LAN2	-	192.168.88.84	255.255.255.192	192.168.88.65		8038
IP камера 15_ LAN2	-	192.168.88.85	255.255.255.192	192.168.88.65		8039
IP камера 16_ LAN2	-	192.168.88.86	255.255.255.192	192.168.88.65		8040
IP камера 17_ LAN2	-	192.168.88.87	255.255.255.192	192.168.88.65		8041
IP камера 18_ LAN2	-	192.168.88.88	255.255.255.192	192.168.88.65		8042
IP камера 19_ LAN2	-	192.168.88.89	255.255.255.192	192.168.88.65		8043
IP камера 20_ LAN2	-	192.168.88.90	255.255.255.192	192.168.88.65		8044
IP камера 21_ LAN2	-	192.168.88.91	255.255.255.192	192.168.88.65		8045
IP камера 22_ LAN2	-	192.168.88.92	255.255.255.192	192.168.88.65		8046
IP камера 23_ LAN2	-	192.168.88.93	255.255.255.192	192.168.88.65		8047
IP камера 24_ LAN2	-	192.168.88.94	255.255.255.192	192.168.88.65		8048
Директор_ LAN3		192.168.88.135	255.255.255.240	192.168.88.129		Fa0/2
Заст дир.._LAN3	-	192.168.88.136	255.255.255.240	192.168.88.129		Fa0/3
Секретар_LAN3	-	192.168.88.137	255.255.255.240	192.168.88.129		Fa0/4
Гол. Бух._LAN3	-	192.168.88.138	255.255.255.240	192.168.88.129		Fa0/5
Ком. Від. 1_LAN3	-	192.168.88.139	255.255.255.240	192.168.88.129		Fa0/6
Ком. Від. 2_LAN3	-	192.168.88.140	255.255.255.240	192.168.88.129		Fa0/7
Каса_ LAN3	-	192.168.88.141	255.255.255.240	192.168.88.129		Fa0/8

Фін. Сл. 1_LAN3	-	192.168.88.142	255.255.255.240	192.168.88.129		Fa0/9
Вузол розр 1_LAN4	-	192.168.88.112	255.255.255.224	192.168.88.97		Fa0/10
Вузол розр 2_ LAN4	-	192.168.88.113	255.255.255.224	192.168.88.97		Fa0/11
Вузол розр 3_ LAN4	-	192.168.88.114	255.255.255.224	192.168.88.97		Fa0/12
Вузол розр 4_ LAN4	-	192.168.88.115	255.255.255.224	192.168.88.97		Fa0/13
Вузол розр 5_ LAN4	-	192.168.88.116	255.255.255.224	192.168.88.97		Fa0/14
Менеджер1_ LAN4	-	192.168.88.117	255.255.255.224	192.168.88.97		Fa0/15
Менеджер2_ LAN4	-	192.168.88.118	255.255.255.224	192.168.88.97		Fa0/16
Менеджер3_ LAN4		192.168.88.119	255.255.255.224	192.168.88.97		Fa0/17
Менеджер4_ LAN4	-	192.168.88.120	255.255.255.224	192.168.88.97		Fa0/18
Менеджер5_ LAN4	-	192.168.88.121	255.255.255.224	192.168.88.97		Fa0/19
Менеджер6_ LAN4	-	192.168.88.122	255.255.255.224	192.168.88.97		Fa0/20
Менеджер7_ LAN4	-	192.168.88.123	255.255.255.224	192.168.88.97		Fa0/21
Менеджер8_ LAN4	-	192.168.88.124	255.255.255.224	192.168.88.97		Fa0/22
Менеджер9_ LAN4	-	192.168.88.125	255.255.255.224	192.168.88.97		Fa0/23
Менеджер10_ LAN4	-	192.168.88.126	255.255.255.224	192.168.88.97		Fa0/24
Сис_адмін_ LAN5	-	192.168.88.149	255.255.255.248	192.168.88.145		Fa0/1
Server_ LAN5	-	192.168.88.150	255.255.255.248	192.168.88.145		Fa0/2
Prihodko_Router_12	Fa0/0	192.168.88.1	255.255.255.192	-		-
	Fa0/1	192.168.88.65	255.255.255.224	-		-
	S0/0/0	10.0.12.1	255.255.255.252	10.0.12.2		
Prihodko _Router_34	Fa0/0	192.168.88.129	255.255.255.240	-		-
	Fa0/1	192.168.88.97	255.255.255.224	-		-
	S0/0/0	10.0.12.5	255.255.255.252	10.0.12.6		-
Prihodko _Router_5	Fa0/1	10.0.12.2	255.255.255.252			
	Fa0/2	10.0.12.6	255.255.255.252	-		-
	Fa0/3	192.168.88.145	255.255.255.248	-		-
	S0/0/0	10.0.12.9	255.255.255.252	10.0.12.10		
Prihodko _ Firewall_1	Fa0/0	10.0.12.10	255.255.252.252	-		-
	S0/0/0	209.165.200.4	255.255.255.252			-

Порти для доступу до камери:

1. 80 - веб-інтерфейс;

2. 554 - RTSP-порт для прямого отримання потоку з камери;

3. 8000 - SDK-порт, необхідний для підключення до ПО IVMS і реєстраторам;

4. 8200 - порт даних, сервісний порт. Визначається автоматично (порт №4 = порт №3 +200).

В налаштуваннях камери порти можна змінити на інші. Це може бути необхідно, якщо в одній локальній мережі знаходиться декілька пристроїв, що вимагають для себе окремі порти. Наприклад, якщо на першій камері порти 80, 554, 8000 і 8200, то на другій камері необхідно проставити порти 81, 555, 8001 і 8201. Після проброса портів за своєю зовнішньою IP-адресою можна зайти на пристрій з Інтернету в вікні браузера. При зміні 8000 порту на інший, порт 8200 зміниться автоматично (порт №4 = порт №3 +200).

Ці IP-адреси будуть використовуватися при виконанні частини з налаштування обладнання мережі.

4.2 Розробка моделі та перевірка роботи комп'ютерної системи

Програмне рішення Cisco Packet Tracer дозволяє імітувати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д. Робота з інтерактивним симулятором дає вельми правдоподібне відчуття налаштувань реальної мережі, що складається з десятків або навіть сотень пристроїв. Налаштування, в своючергу, залежать від характеру пристроїв: одні можна налаштувати за допомогою командопераційної системи Cisco IOS, інші - за рахунок графічного веб-інтерфейсу,треті - через командний рядок операційної системи або графічні меню.

Завдяки такій властивості Cisco Packet Tracer, як режим візуалізації,користувач може відстежити переміщення даних по мережі, поява ізміна параметрів IP-пакетів при проходженні даних через мережевіпристрої, швидкість і шляхи переміщення IP-пакетів. Аналіз подій, що відбуваютьсяв мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

Модель розроблюваної мережі показана на рисунку 4.1.

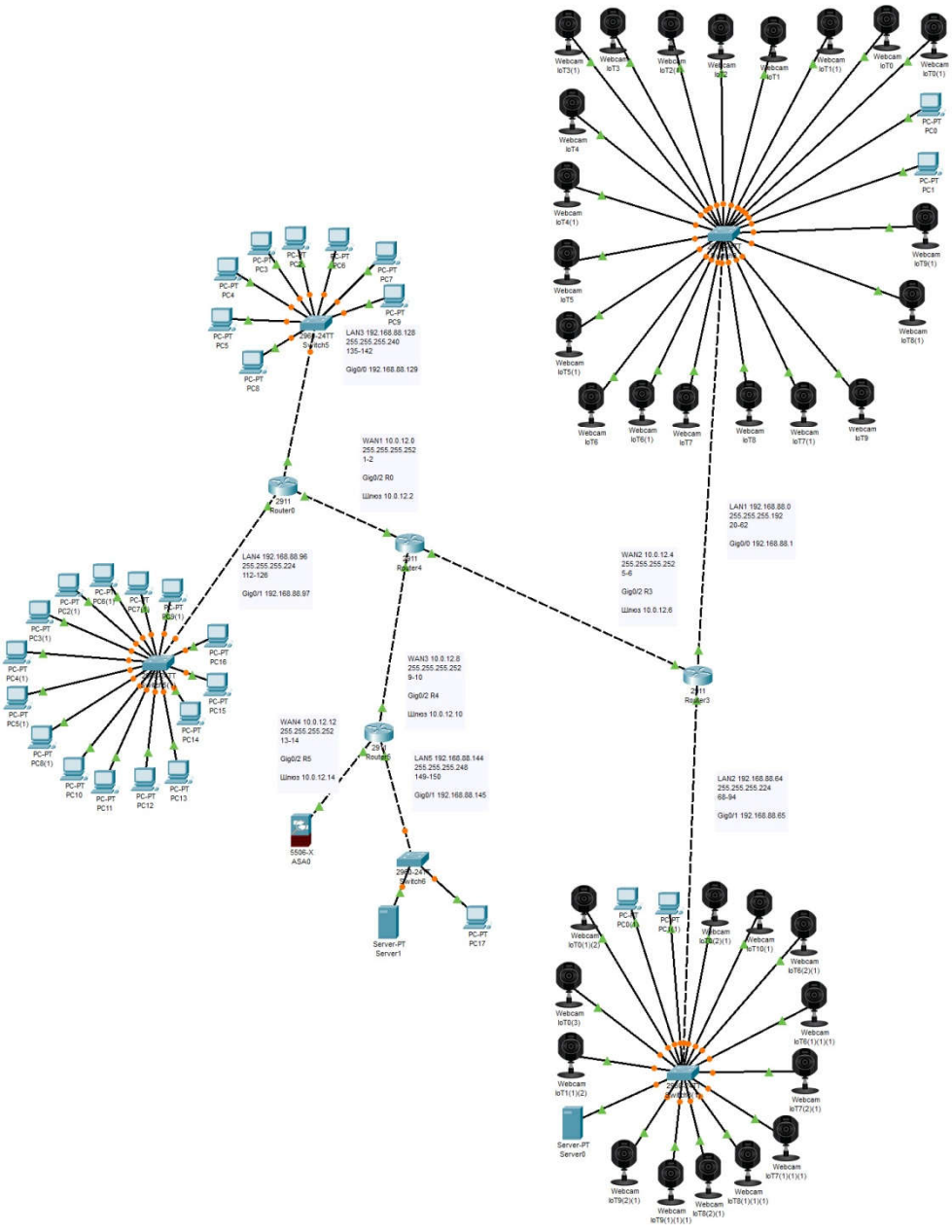

Рисунок 4.1 – Схема моделі мережі

Необхідно вказати на відмінності моделі від проекту, який був розроблений в розділі 3. Головна відмінність у тому, що для спрощення моделі у мережах LAN1 і LAN2 було зменшено кількість камер. В цілому камерам присвїна адресація, що відповідає таблиці 4.4, але пропущені адреси, які розташовані всередині діапазону.

Що до маршрутизації в моделі використано 4 маршрутизатора. Це реалізовано за рахунок використання додаткової мережі WAN.

Наведені відмінності не вплинули на можливості дослідження створеного проекту мережі.

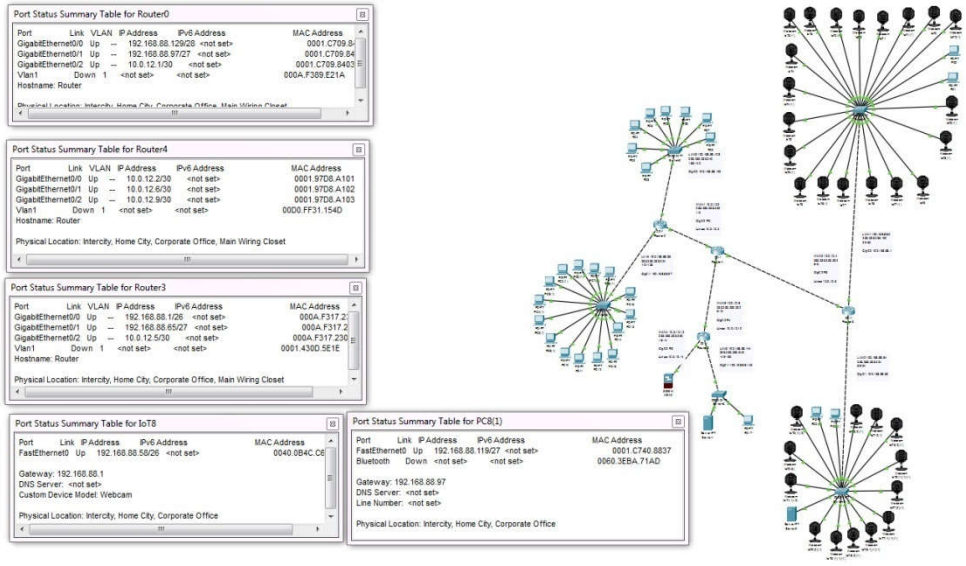

Рисунок 4.2 – Статус пристроїв моделі

Налаштування маршрутизації проводиться статичним методом. Компанія в найближчому часі не буде поширюватися. Для налаштування маршрутизації потрібно прописати шляхи пакетів. Налаштувати маршрут за замовченням. Після налаштування всі вузли в віддалених мережах досяжні між собою і мають шлях в Internet.

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

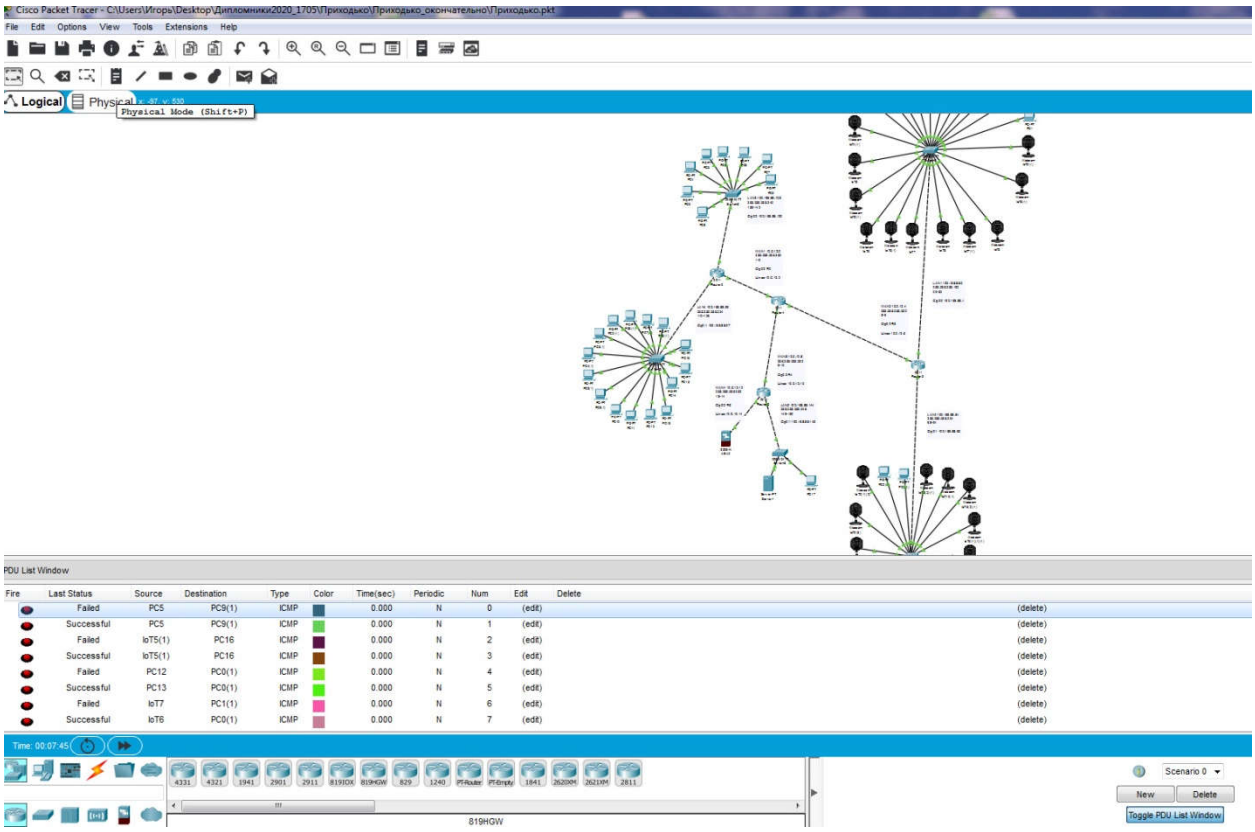

Рисунок 4.3 – Перевірка проходження пакетів між елементами моделі

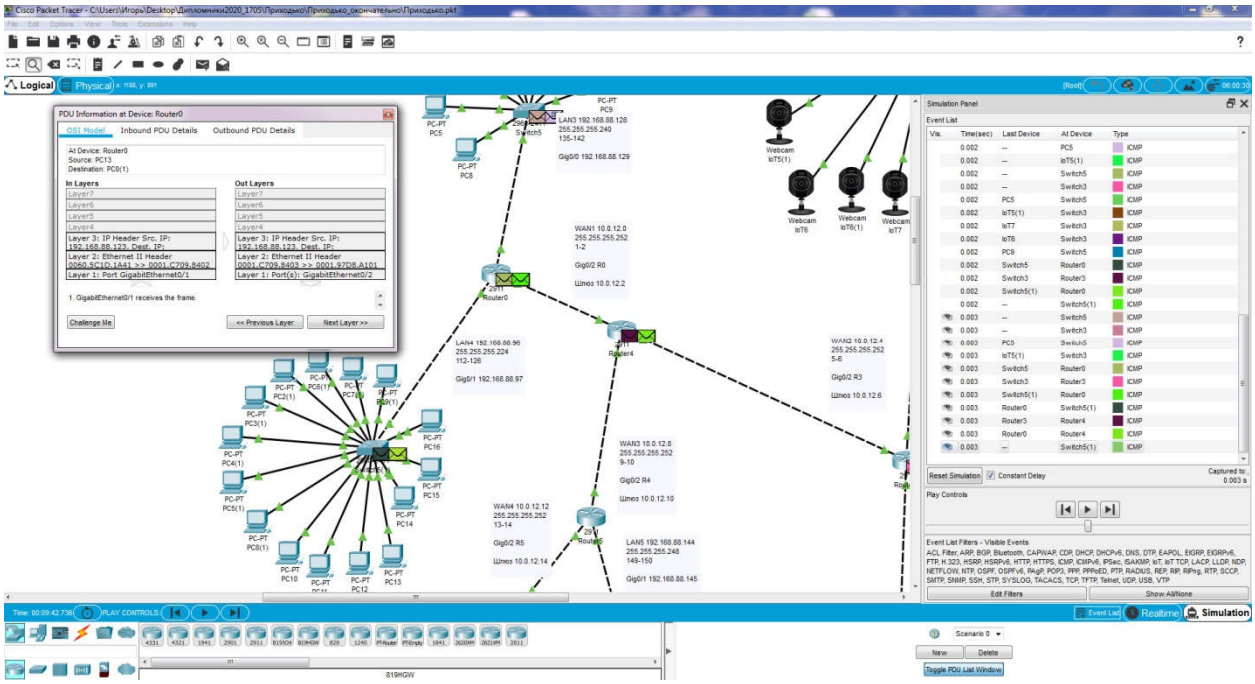

Рисунок 4.4 – Режим симуляції

4.2.1 Базове налаштування конфігурації пристроїв

Комутатор L2 GigabitEthernetPoED-linkDGS-3120-48PC.

Функції управління. Системою можна управляти локально через консольний порт на передній панелі, або віддалено, використовуючи Telnet. Користувач також може управляти комутатором через Web-інтерфейс за допомогою Web-браузера. Кожному комутатору повинна бути призначена IP-адреса, що використовується для взаємодії з мережевим менеджером SNMP або іншими додатками TCP/IP (наприклад, BOOTP, TFTP). IP-адреса комутатора за замовчуванням - 10.90.90.90. Користувачі можуть змінити IP-адресу комутатора за замовчуванням для відповідності схемі адресації мережі.

Управління на основі Web-інтерфейсу. Після успішної установки вона може змінювати комутатор, стежити за його станом за допомогою панелі індикаторів і переглядати статистику в Web-браузері, наприклад, в Netscape Navigator (версії 6.2 і вище) або Microsoft® Internet Explorer (версії 5.0 і вище). Щоб використати Web-інтерфейс потрібно наступне обладнання: Комп'ютер з інтерфейсом RJ-45. Стандартний кабель Ethernet.

Щоб війти доя Web-інтерфейсу комп'ютеру повинна бути призначена IP-адреса з того ж діапазону, в якому знаходиться IP-адреси комутатора. Наприклад, якщо комутатору призначені IP-адреси 10.90.90.90 і маска підмережі 255.0.0.0, то комп'ютеру повинні бути призначені IP-адреси виду 10.x.y.z (де x y - це число від 0 до 255, z - число від 1 до 254) і маска. Введіть IP-адресу 10.90.90.90 в адресному рядку Web-браузера.

Після появи вікна аутентифікації залиште ім'я користувача і пароль порожніми. Потім натисніть OK, щоб перейти до головного вікна налаштувань. IP-адреса комутатора за замовчуванням 10.90.90.90, маска підмережі - 255.0.0.0, шлюз за замовчуванням - 0.0.0.0.

Роутер CiscoRV345P-K9-G5

Майстер установки і диспетчер пристроїв підтримуються браузерами MicrosoftInternetExplorer, MozillaFirefox, AppleSafari і GoogleChrome. Щоб

налагодити пристрій за допомогою майстра установки виконуються наступні дії.

Увімкніть живлення ПК, підключеного до порту LAN1. ПК стає DHCPкліентом пристрою і отримує IP-адресу з діапазону 192.168.1.xxx. Відкрийте веб-браузер. В адресному рядку введіть IP-адресу пристрою за умовчанням: https://192.168.1.1. Відображається повідомлення про сертифікат безпеки сайту. Cisco RV340/RV345/RV345P використовує сертифікат безпеки. Це повідомлення відображається тому, що даний пристрій невідомо вашого комп'ютера. Для продовження натисніть Продовжити відкриття веб-сайту. Відкривається сторінка входу. Введіть ім'я користувача і пароль. Ім'я користувача за замовчуванням - cisco. Пароль за замовчуванням - cisco. Паролі вводяться з урахуванням регістра символів. Клацніть Log In (Вхід в систему). Запускається майстер установки маршрутизатора. Налаштуйте свій пристрій, слідуючи інструкціям на екрані. Майстер установки маршрутизатора повинен виявити і налаштувати ваше підключення. Якщо цього не вдається зробити, інформація про підключення до Інтернету може бути запрошена у користувача. За додатковою інформацією зверніться до інтернет-провайдера. Змініть пароль згідно з інструкціями майстра установки маршрутизатора або описаної в розділі «Зміна імені користувача та пароля адміністратора». Увійдіть в пристрій, використовуючи нові ім'я користувача та пароль. Рекомендується змінити вихідний пароль. Пароль слід змінити до вирішення таких функцій, як дистанційне керування.

Налаштування IP камер. Всі пристрої HIKVISION з останньою прошивкою (IPC версія V5.3.0, DVR/NVR версія V3. 3.0) більше не використовують пароль за замовчуванням. При використанні цих пристроїв в перший раз, користувачеві необхідно активувати пристрій шляхом примусової установки пароля.

Це можна зробити 4-я способами:

- через утиліту SADP (в комплекті поставки)

- через Веб браузер

- через клієнта iVMS-4200 (в комплекті поставки)

- активувати камери за допомогою відеореєстратора.

Якщо все правильно підключили, то в програмі з'явитися список всіх пристроїв Hikvision.

Вибрати пристрій, який потрібно активувати в списку " Онлайн пристроїв ";

- Встановити новий пароль в поле " Device Activation ";

- Підтвердити новий пароль;

- Натиснути на кнопку [OK], щоб активувати пристрій.

Разом з тим, в цій утиліті можна задати/змінити відповідно до вашої мережі ip адресу, шлюз, маску підмережі.

В даному випадку, у вас є прямий доступ з інтернет, ви можете налаштувати маршрутизацію в роутері (NAT) таким чином, що б перенаправити пакети з зовнішньої мережі на внутрішню до необхідних портів (так званий «проброс портів»). «Проброс» повинен бути «дзеркальним» (наприклад з порту 8000 на порт 8000 локальної мережі), в іншому випадку, підключення може працювати не коректно. Порти необхідні для доступу до обладнання:

• 80вебінтерфейс.

• 443для доступу поHTTPS.

• 554RTSPпорт для прямого отримання потокуз камери.

• 8000SDKпорт,для підключення до ПОIVMSi реєстраторів.

• 8200дані,сервісний порт.

Для отримання прямого доступу до камери потрібно налаштувати роутер способом "проброса" на ньому портів або "маршрутизації". Налаштування роутера (NAT) виконується за інструкцією від виробника маршрутизатора. У загальних рисах це виглядає наступним чином.

Заходьте на внутрішній IP роутера ("192.168.0.1", або "10.0.0.1", або будь-який інший, він вказаний в інструкції до роутера), вводите логін і пароль (стандартний логін і пароль вказаний на нижній частині роутера).

Знаходьте пункт "Налаштування NAT/DNAT"/"Port forwarding"/"Віртуальний сервер".

4.2.2Налаштування мереж, комутаторів та адресації IP камер

Необхідна для роботи швидкість інтернет-каналу залежить від трьох параметрів:

- Роздільна здатність камери.
- Частота кадрів.
- Якість зображення (ступінь стиснення).

Керуючи цими трьома параметрами, можна підібрати оптимальний баланс між якістю зображення і споживанням трафіку.

При частоті 25 кадрів/сек для зазначених варіантів стандартного дозволу і якості зображення (ступеня стиснення) вимоги до інтернет-каналу для однієї камери будуть наступні:

Якість зображення	Рекомендована швидкість
1280x720 (1Мрх) /25к/с	1 Мбит/с
1920x1080 (2Мрх) /25к/с	2 Мбит/с
2048x1536 (3Мрх) /25к/с	2 Мбит/с
2592x1728 (4Мрх) /25к/с	2 Мбит/с

Варто враховувати, що камера споживає інтернет-трафік тільки при перегляді онлайн-відео, записи архіву в хмару і спрацьовуванні детектора руху або звуку зі збереженням подій в хмарі.

Коли відео з камер не запитується і запис в хмару не ведеться, трафік складає менше 1 Мб в тиждень (обмін службовою інформацією вашого сервера з дата-центрами).

Ці цифри важливі для ознайомлення з управлінням мережевим навантаженням. Наприклад, 1 камера з високим бітрейтом 8000 Кбіт/с (або 8 Мбіт/с) не приносить проблем в мережі 10/100. А ось 10 камер з такою ж швидкістю передачі даних вимагають смуги 80 Мбіт/с, що становить 80%

використання в локальній мережі 10/100 LAN. Цього достатньо, щоб побачити помітне уповільнення відеозапису, і можуть виникнути деякі проблеми, особливо - якщо локальна мережа використовується не тільки для передачі відео в системі відеоспостереження підприємства.

Перемикання на Gigabit LAN це 8% -від використання мережі. Завжди потрібно перевіряти можливості мережі, в яку інтегрована система відеоспостереження. При використанні IP-камер завжди використовуйте гігабітні маршрутизатори і комутатори, всюди - де це тільки можливо. Крім того, переконайтеся, що ваш мережевий відеореєстратор підключений саме до гігабітних входів комутатора.

Формула для розрахунку пропускної здатності локально обчислювальної мережі:

$L=X \cdot N \cdot M \cdot F$,

де X - це змінна, яка залежить від ступеня стиснення відео і рівня активності руху в кадрі. При використанні кодека h264 будемо вважати, що це значення дорівнює:

0,03 (низька)

0,06 (середня)

0,09 (висока)

N - кількість камер.

M – роздільна здатність в мегапикселях кожної камери, 4 Мегапикселя.

F - Кадрів в секунду. Наша камера працює з частотою 25 кадрів в секунду.

Для однієї камери необхідна пропускна здатність мережі не менша ніж 9 Мбіт/сек. Для 63 камер мережа повинна мати пропускну здатність не менш ніж 567 Мбіт/сек. Враховуючи, що до цих мереж підключені ще й термінали охорони необхідно використовувати гігабітну мережу.

4.3 Налаштування роботи Інтернет

Розглянемо докладніше налаштування апаратного шлюзу ZyWALL USG для підключення до Інтернету при використанні статичної IP-адреси.

В меню **Configuration> Network> Interface> Ethernet** для налаштування статичної IP-адреси на WAN-інтерфейсі пристрою (по запису конфігурації WAN-інтерфейсу і потім натисніть Edit).

Увікні**EditEthernet**врозділі**IPAddressAssignment**встановіть**UseFixedIP Address**. Вполї**IPAddress**вкажітьстатичнуIP-адресу, виданупровайдером, вполе**SubnetMask** - маскупідмережіівполі**Gateway** - IP-адресушлюзу. НатиснітькнопкуOKдлязбереженняналаштувань.

Необхідно перевірити, щобвменю**Configuration>Network>Interface>Trunk**буввключенийпараметр **EnableDefaultSNAT**
(длянаданнякористувачамлокальноїмережізвнутрішніmиIP-адресамидоступудомережіІнтернет).
ДлявідображенняцьогопараметрувлівомуверхньомукуткунатиснітьShowAdvancedSettings. За замовчуванням **Enable Default SNAT** включений.

Для налаштувань IP-адреси DNS-сервера зайдіть в меню **System> DNS**.

У розділі **Domain Zone Forwarder** натисніть Add для створення нового запису. В поле **Domain Zone** можна вказати доменну зону. Наприклад, zyxel.com.tw є доменною зоною для доменного імені www.zyxel.com.tw. Введіть символ * (зірочка), якщо всі доменні зони обслуговує DNS-сервер.

В поле Public DNS Server вкажіть IP-адресу DNS-сервера (значення 0.0.0.0 використовувати не можна). Натисніть кнопку OK для збереження налаштувань.

Якщо в мережі провайдера існує прив'язка по MAC-адрес (провайдер вимагає певну MAC-адресу для надання доступу до Інтернету), налаштуйте клонування MAC-адреси в ZyWALL USG.

У розділі **MAC Address Setting** встановіть значення **Overwrite Default MAC Address** і потім натисніть кнопку **Clone by host** (Клонувати з хоста).

Зайдіть в меню **Configuration> Network> Interface> Ethernet** для налаштування статичної IP-адреси на WAN-інтерфейсі пристрою (клацніть по запису конфігурації WAN-інтерфейсу і потім натисніть Edit).

У вікні **Edit Ethernet** в лівому верхньому кутку натисніть **Show Advanced Settings** для відображення додаткових параметрів.

У вікні **Clone MAC Address** вкажіть IP-адресу комп'ютера, з якого ви хочете клонувати MAC-адресу, щоб на WAN-інтерфейсі замінити MAC-адресу апаратного шлюзу (використовується за умовчанням) зазначеним MAC-адресою мережевого адаптера.

Натисніть кнопку OK для продовження. Потім ви побачите, що в поле **Overwrite Default MAC Address** була додана MAC-адресамережевого адаптера комп'ютера. Саме цим зазначеним MAC-адресою апаратний шлюз ZyWALL USG буде підміняти свою власну (встановлену за замовчуванням) MAC-адресу.

4.4 Розрахунок основних характеристик для вихідного трафіку найбільшого сегмента мережі підприємства

Розрахувати основні характеристик для вихідного трафіку в найбільшому сегменті мережі підприємства за умови, що 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.

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

Дано:

кількість вузлів в найбільшій мережі: 15

середня інтенсивність трафіку: μ=160 (кадрів/с)

середня довжина повідомлення: l=600 байт;

вимоги до затримки передачі пакету – ≤5 мс.

Згідно кількості вузлів (15) для їх підключення на рівні розподілу обираємо роутер CiscoRV320-K9-G5. (1 шт), на рівні доступу комутатор L3 FastEthernetCiscoSF500-24-K9-G5 (1 шт).

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною 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 μ=160 (кадрів/с), а середня довжина повідомлення – 600 байт.

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

Рр.д= μ·l·n·8=160·600·24·8= 18,4 (Мбіт/с), де

n- кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином. Так як до одного роутера рівня розподілу підходять 2 комутатори рівня доступу, а загальна кількість користувачів дорівнює 23, то пропускна здатність мережі на рівні розподілу буде дорівнює:

Рр.р= μ·l·N·8=160·600·48·8= 36.9 (Мбіт/с), де

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

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

Загальне навантаження на комутатор не повинно перевищувати:

μвих=1000 000 000/(600*8)=208334 пакетів/с

Оскільки кожне джерело виробляє в середньому 160 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

N=208334/160=1302 джерел.

Що задовольняє нашу мережу на 23 ПК.

Кожен з 23 ПК посилає потік заявок з інтенсивністю 160 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів:

λ=N·μ= 23*160=3680 (пакетів/с)

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

ρ=λ/μ_вих =3680/208334=0,017

Коефіцієнтзайнятостікомутаторарівнярозподілу:

r=ρ/(1-ρ)=0,017/(1-0,017)=0,017

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

$$T=1/((\mu-\lambda))=1/(208334-3680)=4.9\cdot10^{-6}\ с$$

Середня довжина черги:

L_чер=ρ^2/(1-ρ)= ⟦0,017^2/(1-0,017)=0,0017

Ця цифра може бути корисною при налаштуванні черг на обладнанні - в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне; воно свідчить про те, що система працює з великим запасом по продуктивності.

Середній час перебування пакета в черзі

T_оч=L_чер/λ=0,0017/3680=0,046 мкс

Це значення менше необхідного значення ≤5 мс, що задовольняє вимогам.

Пропускна здатність каналу:

λ =(пропускна здатність)/(довжина кадру)=b/l

b=λ·l=3680·600·8=13200000біт/с=13.2Мбіт/с

Що задовольняє пропускній здатності вихідного каналу в 1000Мбіт/с.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Розрахунок капітальних витрат пов'язаних з впровадженням системи відеонагляду

Розрахуємо капітальні витрати, пов'язані з виготовленням та впровадженням компютерної мережі напідприємстві.

Визначення проектних капітальних витрат проводиться за такою формулою

$$К_{пр} = С_{об} + Д_{тр} + М_{мн} + К_{пз} \quad (5.1)$$

де $С_{об}$ – витрати на комплектуючі вироби;

$Д_{тр}$ – витрати на транспортно-заготівельні витрати;

$М_{мн}$ – витрати на монтаж і налагодження системи;

$К_{пз}$ – витрати на програмне забезпечення.

Витрати на розробку систем відеоспостереження та контролю доступом визначаються за формулою (5.2):

$$К_{пр} = З_{в}\ t, \quad (5.2)$$

де $З_{в}$ – 70ідео спостереже заробітна плата спеціаліста з розробки, 70іде / годину;

t – загальна тривалість розробки та впровадження систем 70ідео спостереження та контролю доступом, годин.

Середньогодинна заробітна плата спеціаліста з розробки складає 35 грн/годину.

Загальна тривалість розробки та впровадження систем 70ідео спостереження та контролю доступом визначається за формулою (5.3):

$$t = t_{обс} + t_{мз} + t_{тз} + t_{пз}, \quad (5.3)$$

де $t_{обс}$ – тривалість проведення обстеження ОІД, годин;

$t_{мз}$ – тривалість розроблення моделі загроз для ІзОД, годин;

$t_{тз}$– тривалість розроблення технічних завдань на створення систем відеоспостереження та контролю доступом , годин;

$t_{пз}$– тривалість розроблення пояснювальної записки з створення систем відеоспостереження та контролю доступом, годин.

$$t = 6 + 3 + 6 + 4 = 19 \text{ годин}$$

Витрати на розробку систем відеоспостереження та контролю доступом:

$$К_{пр} = 35 \ \ 19 = 665 \text{ грн.}$$

Витрати на обладнання, призначеного для вдосконалення систем відеоспостереження та контролю доступом в ТОВ «Вітязь» представлені в таблиці 5.1

Таблиця 5.1 – Вартість обладнання, призначеного для вдосконалення систем відеоспостереження та контролю доступом

Назва	Ціна, грн	Кількість	Загальна ціна, грн
Мережева вулична IP камера HIKVISION	3691	35	129200
Комутатор D-linkDGS-3120-48PC	12800	1	12800
Комутатор Planet GS-4210-24P4C	5826	1	5826
Комутатор *Cisco SG300-20*	12200	1	12200
Комутатор*CiscoSF500-24-K9-G5*	15200	1	15200
Роутер*Cisco RV345P-K9-G5*	7240	2	14480
Роутер Cisco RV320-K9-G5	7631	1	7631
Кабель вита пара		605м	1246
Загальна сума			198788

Отже витрати на обладнання, призначеного для вдосконалення систем відеоспостереження та контролю доступом становлять 198788 грн.

Витрати на встановлення обладнання становлять 19878,8 грн.

Капітальні витрати на проектування та впровадження систем відеоспостереження та контролю доступом :

$$К = 665 + 198788 + 19878,8 = 219331, 8 \text{ грн.}$$

5.2 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на функціонування систем відеоспостереження та контролю доступом визначаються за формулою (5.4):

$$С = С_в + С_к, \qquad (5.4)$$

де $С_в$ – вартість Upgrade-відновлення й модернізації систем, грн.;

$С_к$ – витрати на керування системами в цілому, грн.

Витрати на керування систем відеоспостереження та контролю доступом визначається за формулою (5.5):

$$С_к = С_а + С_з + С_{ел}, \qquad (5.5)$$

де $С_а$ – річний фонд амортизаційних відрахувань, грн.;

$С_з$ – річний фонд заробітної плати охоронця, грн.;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою систем відеоспостереження та контролю доступом протягом року, грн.

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів.

Річний фонд амортизаційних відрахувань:

$$С_а = 219331,8 \quad 0,5 = 109665,9 \text{ грн.}$$

Річний фонд заробітної плати охоронцявизначається за формулою (5.6):

$$С_з = З_{осн} + З_{дод}, \qquad (5.6)$$

де $З_{осн}$, $З_{дод}$– основна і додаткова заробітна плата відповідно, грн. на рік.

Основна заробітна плата визначається, виходячи з місячного

посадового окладу, а додаткова заробітна плата – в розмірі 8% від основної заробітної плати.

Річний фонд заробітної плати охоронця:

$$С_з = 2000 \quad 12 \quad + 0,08 \quad 2000 \quad 12 = 43200 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою систем відеоспостереження та контролю доступом протягом року, визначається за формулою (5.7):

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \qquad (5.7)$$

де Р – встановлена потужність апаратури систем відеоспостереження та контролю доступом, кВт;

$F_р$– річний фонд робочого часу систем відеоспостереження та контролю доступом, годин;

$Ц_е$ – тариф на електроенергію, грн / кВт · годин.

Вартість електроенергії, що споживається апаратурою комплексу технічного захисту інформації протягом року:

$$С_{ел} = 3 \cdot 3120 \cdot 0,9 = 8424 \text{ грн.}$$

Витрати на керування систем відеоспостереження та контролю доступом:

$$С_к = 109665,9 + 43200 + 8424 = 161289, 9 \text{ грн.}$$

Річні експлуатаційні витрати на функціонування систем відеоспостереження та контролю доступом:

$$С = 4000 + 161289,9 = 165289,9 \text{ грн.}$$

Висновок

В економічному розділі даного дипломного проекту був зроблений розрахунок капітальних витрат на проектування та впровадження систем відеоспостереження та контролю доступом. Також був проведений розрахунок річних експлуатаційних витрат на функціонування систем відеоспостереження та контролю доступом, які склали 165289,9 грн. Виходячи з цього, було встановлено, що термін окупності капітальних інвестицій становить один рік.

6 ОХОРОНА ПРАЦІ

6.1 Інженерно-технічні заходи щодо охорони праці на об'єкті

Офіс підприємства розташований в двоповерховій будівлі.Системи каналізації та водопостачання на підприємстві централізовані і виходять за межі контрольованої зони. Система опалення на підприємстві також централізована і відбувається за допомогою опалювальних радіаторів. Система ж вентиляції даного об'єкта.Централізоване електропостачання приміщення здійснюється від трансформаторної електростанції.Система заземлення виконана згідно вимогПравил безпечної експлуатації електроустановок і забезпечує заземлення всіх приладів присутніх на підприємстві на загальний контур заземлення, який виходить за межі контрольованої зони. Також на підприємстві встановлені системи охоронної ті пожежної сигналізації..

6.1.1 Клас приміщення по небезпеці поразки електричним струмом

Клас приміщення по небезпеці поразки електричним струмом – 1, згідно з ПУЭ-85 (без підвищеної небезпеки поразки електричним струмом: сухе, безпилове, з нормальною температурою та з ізольованими підлогами.

6.1.2 Режим нейтралі електричних мереж, застосовуваних на об'єкті

Електричні мережі за режимом нейтралі поділяють на:

– мережі з глухозаземленоюнейтраллю джерела живлення;

– мережі з ізольованою нейтраллю джерела живлення.

На об’єкті застосовується електричні мережі з глухозаземленоюнейтраллю, тому що одну з нейтралей силових трансформаторів заземлено безпосередньо.

6.1.3 Заходи щодо електробезпеки

На даному об’єкті всі заходи щодо електробезпеки повинні виконуватись згідно ГОСТ 12.1.019 «ССБТ. Електробезпека. Загальні вимоги

і номенклатура видів захисту», ГОСТ 12.1.030 «ССБТ. Електробезпека. Захисне заземлення, занулення».

Заходи щодо електробезпеки складаються з технічних засобів та організаційних заходів. Вони спрямовані на забезпечення недоступності до струмопровідних частин та неможливості випадкового дотику до них, усунення небезпеки поразки у замиканні струму на корпус електрообладнання або на землю; запобігання помилкових дій персоналу в електроустановках.

Персонал, який працює в електроустановках, систематично навчають, перевіряють знання і тренують по техніці безпеки [9].

На даномуоб'єктііснуютьнаступнішкідливіфактори:

1) наявність шуму та вібрації;
2) наявність електромагнітного випромінювання;
3) наявність ультрафіолетового та інфрачервоного випромінювання;
4) наявність електростатичного поля;
5) перенапруження зорового аналізатора;
6) монотонність праці;
7) розумове перенапруження.

Для запобігання дії цих шкідливих факторів потрібно:

1) для максимального зниження рівня шуму слід замінити старе обладнання на сучасне, а також здійснювати своєчасну профілактику зносу обладнання;
2) для запобігання електромагнітного випромінювання потрібно дотримуватись правил і режимів при роботі з ЕОТ;
3) для запобігання ультрафіолетового та інфрачервоного випромінювання потрібно застосовувати захисні екрани;
4) для зниження електростатичного поля потрібно застосовувати заземлений захисний екран;

5) для запобігання перенапруження зорового аналізатора потрібно виконувати спеціальну гімнастику для очей, правильно розміщувати персональний комп'ютер;
6) для запобігання монотонності праці необхідно вибирати програмне забезпечення, що зменшує одноманітні операції, використання нових технічних засобів введення;
7) для запобігання розумового перенапруження потрібно дотримання режимів праці і відпочинку.

6.1.4 Протипожежні заходи для об'єкта досліджень

На даному об’єкті присутні не горючі стіни і підлоги, що не підтримують горіння, і стелі, не містять вибухонебезпечних, легкозаймистих або токсичних речовин і матеріалів а також присутні електрообладнання, а відповідно належить до класу «Г» по пожежній безпеці.

У приміщеннях такого класуприсутні:

– система пожежної сигналізації;

– вогнегасники;

– аптечка;

Пожежна профілактика – це комплекс організаційних і технічних заходів, спрямованих на гарантування безпеки людей, запобігання пожежам, обмеження їх поширення, а також створення умов для успішного гасіння пожежі.

Забезпечення пожежної безпеки об'єкта передбачає створення системи попередження пожеж та протипожежного захисту. Велике значення при цьому мають організаційно-технічні заходи, які умовно можна поділити на:

а) організаційні (організація пожежної охорони, навчань, інструктажів та ін.);

б) технічні (суворе дотримання правил і норм, визначених чинними нормативними документами, при реконструкції приміщень, технічному переоснащенні виробництва, експлуатації електромереж, опалення, освітлення та ін.);

в) заходи режимного характеру (заборона паління та застосування відкритого вогню в недозволених місцях та ін.);

г) експлуатаційні (своєчасне проведення профілактичних оглядів, ремонтів устаткування тощо).

З метою попередження пожеж, їх поширення та боротьби з ними усі працівники підприємства ТОВ «Вітязь», проходять навчання та інструктажі з питань пожежної безпеки.

6.2 Розрахунок системи освітлення.

Розрахунок штучного освітлення виконується одним з наступних методів: коефіцієнта використання, питомої потужності чи крапковим. Для розрахунку штучного освітлення потрібно вибрати систему освітлення, джерело світла і світильник, визначити кількість світильників для забезпечення нормованої освітленості і розташувати їх в правильному місці[27].

Розрахунок освітлення проводиться для кімнати комерційного відділу площиною 25м^2, довжина якої 5м, ширина - 5м. Розрахунок буде здійснюватись методом коефіцієнта використання.

Для визначення кількості світильників визначимо світловий потік, який поступає на поверхню за формулою (4.1):

$F=E \cdot S \cdot K \cdot Z\eta$, де (6.1)

F– необхідний світловий потік ламп у кожному світильнику, лм;

E– нормована мінімальна освітленість, лк. У нашому випадку, роботу персоналу можна віднести до розряду точних робіт, отже, мінімальна освітленість буде Е = 300Лк.

k– коефіцієнт запасу, враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщення і характеру проводимих у ньому робіт і в даному випадку згідно за таблицею 5.4 k = 1,5);

S– освітлювана площа, м^2(у нашому випадку S = 25м^2);

z – коефіцієнт мінімальної освітленості (у нашому випадку для люмінесцентних ламп z =1,1);

η– коефіцієнт використання світлового потоку (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в частках одиниці; залежить від характеристик світильника, розмірів приміщення, фарбування стін і стелі, характеризується коефіцієнтами відображення від стін (P_C) стелі ($P_П$), та робочої поверхні ($P_Р$)), значення коефіцієнтів P_C, $P_П$і $P_Р$ були знайдені по таблиці 5.6:

P_C = 50%, $P_П$ = 70%, $P_Р$ = 30%,. Значення η визначимо по таблиці 5.7 коефіцієнтів використання різних світильників. Для цього обчислимо індекс приміщення за формулою (4.2) :

$$I=Sh\cdot(A+B) \quad \text{, де} \qquad (6.2)$$

S – площа приміщення, S = 25 м^2;

h – розрахункова висота підвісу, h = 3.05;

A– ширина приміщення, А = 5 м;

B – довжина приміщення, В = 5 м.

Підставивши значення отримаємо:

$$I=253,05\cdot(5+5)=0,832$$

Знаючи індекс приміщення I, знаходимо η= 0,29

Підставимо всі значення у формулу (6.1) для визначення світлового потоку *F*:

$F=300\cdot25\cdot1,5\cdot1,10,29=42674$ лм

Для освітлення обираємо люмінесцентні лампи типу ЛТБ80-4, потужність яких - 80 Вт, напруга - 102 В, світловий потік після 100 годин

горіння F = 4300 Лк. Розрахуємо необхідну кількість ламп за формулою (6.3):

N - число ламп, яке необхідно визначити;

F - світловий потік, F = *42674* лм;

Fл- світловий потік лампи, Fл = 4300 лм.

Знаходимо N: 10 ламп.

Таким чином, для забезпечення оптимальних умов освітлення робочого місця в комерційному відділі необхідно встановити 10 люмінесцентних ламп обраного типу.

Висновок

У розділі «Охорона праці» розроблено інженерно-технічні заходи щодо охорони праці на об'єкті. Також зроблено розрахунок системи освітлення приміщення комерційного відділу.

ВИСНОВКИ

Кваліфікаційна робота виконана відповідно до теми. В роботі розроблений проект комп'ютерної мережі, яка складається з кількох докальних мереж, дві з яких оснащені IP відеокамерами.

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

Зважаючи на високі темпи розвитку IT індустрії, комплектуючих, алгоритмів і програмних продуктів при проектуванні мережі використано підхід, завдяки якому основні вузли мережі забезпечують пропускну здатність з великим запасом.

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

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

Розроблена модель мережі та досліджена у пакеті Cisco Packet Tracer. Також розраховані параметри трафіку.

Результати досліджень моделі показали можливість використання проекту на підприємстві.

Можливі зміни технічних вимог до мережі і комп'ютерної системи вцілому потребують перегляду розробленої структури.

Виходячи з розрахунку економічних показників, видно, що впровадження нового обладнання комп'ютерної системи є дуже коштовними в матеріальному плані, але необхідними, оскільки впровадження нової комп'ютерної системи дозволить підвищити ефективність функціонування підприємства вцілому.

У кваліфікаційної роботи було розглянуто питання охорони праці при експлуатації комп'ютерної техніки в офісах підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Информационные технологии в менеджменте (управлении): учебник и практикум для академического бакалавриата/ Ю.Д. Романова [и др.]; под общей редакцией Ю.Д. Романовой. — Москва: Издательство Юрайт, 2019. — 478с.

2. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж :[навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.

3. Жуков, І. А. Комп'ютерні мережі та технології : навч. посіб./І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.

4. Аналоговыеицифровыесистемывидеонаблюдения(Електрон. ресурс) / Спосіб доступу: URL:http://elites-montage.com.ua/svanalog.php. - Загол. з екрана.

5. Система відеоспостереження (Електрон. ресурс) / Спосіб доступу: URL: http://fidgur.livejournal.com/29944.html – Загол. з екрана.

6. Формати відеоспостереження (Електрон. ресурс) / Спосіб доступу: URL: http://spec.prom.ua/a37913-klassifikatsiya-formatov-razresheniya.html – Загол. з екрана.

7. Закон України "Про електронний цифровий підпис", 2003 – 10 с.

8. ГОСТ 2.702-75. ЕСКД. Правила выполнения электрических схем. – М.: Госстандарт, 1995. – 115 с.

9. IP Калькулятор [Электронный ресурс] – Режим доступа : URL : http://ip-calculator.ru/. – Загол. з екрана.

10. VLSM Calculator – калькулятор подсетей с маской переменной длины [Электронный ресурс]. – Режим доступа:URL:http://www.vlsm-calc.net/. – Загол. з екрана.

11. ГОСТ 2.737-68. ЕСКД. Условные графические обозначения в схемах. Устройства связи. – М.: Госстандарт, 1995. – 115 с.

12. Воробьёва Н.И., Корнейчук В.И., Савчук Е.В. Надёжность компьютерных систем. – К.: «Корнійчук», 2002. – 144 с.

13. Мережеве обладнання [Электронный ресурс] – Режим доступа : URL : https://elmir.ua/routers/router_zyxel_sbg5500-a.html. – Загол. з екрану.

14. Классификация угроз информационной безопасности (Електрон. ресурс)/Спосіб доступу:URL:http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml – Загол. з екрана..

15. 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.

16. Гук М.Аппаратные средства IBM PC. – СПб.:Питер, 1997. – 288 с.

17. Кулаков Ю.А., Луцкий Г.М. Локальные сети. – К.: Юниор, 1998. – 336 с.

18. Кулаков Ю.А., Омелянский С.В. Компьютерные сети. Выбор, установка, использование и администрирование. – К: Юниор, 1999. – 544 с.

19. Спортак М, Паппас Ф., Рензинг Э. Компьютерные сети. Книга 1. Энциклопедия пользователя: Пер. с англ. – М.: Диасофт, 1998. – 432 с.

20. Баня Е.Н. Компьютерные сети. – К.: Світ, 1999. – 112 с.

21. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 172 с.

22. Джеймс Челлис Основы построения сетей: Учебное пособие для специалистов MCSE 1.0. – СПб.: Питер, 1997. – 326 с.

23. Microsoft Corporation. Принципы проектирования и разработки программного обеспечения. Учебный курс MSCD/ Пер. с англ. – М.: Издательско-торговый дом «Русская редакция», 2002. – 736 с.

24. 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.

25. 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.

26. 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.

27. Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186с.

28. В.І. Голінько,В.Ю. Фрундін, Я.Я. Лебедєв, В.Є. Колесник Методичні вказівки з виконання розрахункової частини розділу „Охорона праці”в дипломних проектах студентів інституту електроенергетики. Частина 1 – Дн.: Редакційно-видавничий комплекс, 2004 - 37 стр.

Додаток А

Тексти програм налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20005-01 12 01

Листів 7

2020

АНОТАЦІЯ

Даний документ містить ПЗ налаштувань маршрутизаторів Cisco для структурної схеми моделі комп’ютерної системи.

Тексти програм реалізовані на мові конфігураційних скриптів для мережного обладнання Cisco.

Середовище розробки та налагодження скриптів – пакет моделювання - мереж Cisco Packet Tracer в середовищі операційної системи Windows 7.

ЗМІСТ

1. **Скрипт налаштування Router1**

```
!
interface GigabitEthernet0/0
 ip address 192.168.88.129 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.88.97 255.255.255.224
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.0.12.1 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 network 192.168.88.96 0.0.0.31
 network 192.168.88.176 0.0.0.15
 network 10.0.12.0 0.0.0.3
```

2. **Скрипт налаштування Router2**

```
interface GigabitEthernet0/0
 ip address 10.0.12.10 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.88.145 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.0.12.13 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router eigrp 100
 redistribute static
 network 192.168.88.144 0.0.0.7
 network 10.0.12.8 0.0.0.3
 network 10.0.12.12 0.0.0.3
```

3. Скрипт налаштування Router3

```
interface GigabitEthernet0/0
 ip address 192.168.88.1 255.255.255.192
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.88.65 255.255.255.224
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.0.12.5 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 network 192.168.88.0 0.0.0.63
 network 192.168.88.64 0.0.0.31
 network 10.0.12.4 0.0.0.3
```

4. Скрипт налаштування Router4

```
interface GigabitEthernet0/0
 ip address 10.0.12.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.0.12.6 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 10.0.12.9 255.255.255.252
```

```
 duplex auto
 speed auto
!
interface GigabitEthernet0/2/0
 ip address 8.8.8.10 255.0.0.0
!
interface Serial0/3/0
 no ip address
 clock rate 2000000
!
interface Serial0/3/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 100
 redistribute static
 network 10.0.12.0 0.0.0.3
 network 10.0.12.8 0.0.0.3
 network 10.0.12.4 0.0.0.3

!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/3/0
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/2/0
```