Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи бакалавра

**студента** Оболонська Анна Олександрівна
(ПІБ)

**академічної групи** 123-20з-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:** «*Кіберфізична система охорони периметра промислового підприємства ТОВ «Оптиматех» з детальним опрацюванням побудови та налаштування корпоративної мережі»*

Виконавець: студент 3 курсу, групи 123-20з-1 _____ Оболонська А.О.
(підпис) (прізвище та ініціали)

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинг. | інституційною | |
| Кваліфікаційної роботи | Доц. Сергєєва К.Л. | | | |
| Розділів: | | | | |
| Загальна частина | Доц. Сергєєва К.Л. | | | |
| Розробка корпоративної мережі | Ас. Панферова Я.В. | | | |
| Розробка апаратної частини | Доц. Бешта Д.О. | | | |
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | Проф.Цвіркун Л.І. | | | |

**Дніпро**
**2024**

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

_____
"____" _____ 2024 р.

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

**студенту групи** *123-20з-1* *Оболонській Анні Олександрівні*
(група) (прізвище, ім'я та по батькові)

**Тема дипломної роботи** «*Кіберфізична система охорони периметра промислового підприємства ТОВ «Оптиматех» з детальним опрацюванням побудови та налаштування корпоративної мережі»*

*затвержена наказом ректора НТУ "Дніпровська політехніка"*
*від « » 2024 р. № - 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 ТОВ «Оптиматех» з детальною розробкою комп'ютерної мережі.* | *15.03.2024 р.* |
| ***Технічні вимоги до компютерної системи*** | *На основі аналізу особливостей і потреб підприємства сформулювати технічні вимоги до розробки комп'ютерної системи охорони периметру.* | *01.04.2024 р.* |
| ***Розробкак корпоративної мережі*** | *Розв'язати завдання з розробки комп'ютерної мережі ТОВ «Оптиматех» з опрацюванням апаратного забезпечення.* | *15.05.2024 р.* |
| ***Графічна частина*** | *Графічні результати розробки системи подати у вигляді рисунків, таблиць, схем та креслень на 10 арк. формату А4.* | *20.05.2024 р.* |

Завдання видав, кер. роботи _____ доц. Сергєєва К.Л.
(підпис)

Завдання прийняв до виконання _____ Оболонська А.О.
(підпис)

Дата видачі завдання « » *.2024 р.*
Термін подання дипломної роботи до ДЕК 2*0.05.2024 р.*

# РЕФЕРАТ

Пояснювальна записка: 92 с., 30рис., 5 табл., 1додаток, 24джерела. КОМПЮТЕРНА, СИСТЕМА, МЕРЕЖА, ОХОРОНА, ПЕРИМЕТР, МОДЕЛЬ, НАЛАШТУВАННЯ

Об'єкт розробки: корпоративна комп’ютерна мережа що забезпечує роботу комп’ютерної системи ТОВ «Оптиматех» та системи охорони периметра промислового підприємства.

Мета: забезпечення ТОВ «Оптиматех» сучасними мережевими засобами, які дозволять підприємству бути конкурентноспроможним в сучасному, динамічному ринку.

Розроблені технічні вимоги до комп’ютерної мережі та інформаційної системи підприємства.

Проведено аналіз сучасного мережевого обладнання та тенденцій розвитку мережевих технологій. На основі чого обрано технічні засоби організації комп’ютерної мережі, системи охорони периметру.

Розроблена адресація усіх пристроїв інформаційної системи. Виконано моделювання розробленої мережі в середовищі CiscoPacketTracer. Симуляція роботи мережі підтвердила що виконані розрахунки та налаштування вірні і мережа працездатна.

Кваліфікаційна робота бакалавра виконана відповідно до існуючих вимог та теми.

Результати кваліфікаційної роботи оформлені у вигляді пояснювальної записки з додатками.

# ЗМІСТ

# ПЕРЕЛІК УМОВНХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

ІТ – інформаційні технології;

ІОД – інформація з обмеженим доступом;

ТОВ – товариство з обмеженою відповідальністю;

АРМ – автоматизоване робоче місце;

КІСП – комп’ютерна інформаційна система підприємства;

ЛОМ – локальна обчислювальна мережа;

ЦП – цифровий підпис;

СКУД – система контролю управління доступом;

СОП – система охорони периметра.

# ВСТУП

Хімічна промисловість є окремою дуже важливою галузю у світовій промисловості. Перші підприємства були засновані ще 1740 р. у Великій Британії (Річмонд), 1766 р. мови у Франції (Руан), 1810 р. у Німеччині (Лейпциг).

Інфраструктурні фактори включають наявність інженерних комунікацій (автодоріг, електромереж, каналізації та водопроводу та ін.) та забезпечують стабільне функціонування самого виробництва та зв'язок його з постачальниками сировини та споживачами готової продукції.

При функціонуванні виробництва необхідно обов'язково враховувати фактори безпеки. Усі підприємства хімічної галузі промисловості належить до небезпечних видів виробництв, оскільки негативно впливають на всі компоненти навколишнього середовища. При функціонуванні будь-якого промислового підприємства утворюються відходи - газоповітряні викиди, стічні води та тверді промислові відходи. Після необхідного знешкодження гази викидають в атмосферу, рідкі відходи скидають у каналізацію, тверді та деякі рідкі горючі відходи спалюють у спеціальних печах або захоронюють на спеціально обладнаних полігонах твердих промислових відходів (ТПО). Відходи хімічних виробництв містять речовини I–III класів небезпеки, тому проблема забезпечення захисту навколишнього середовища від негативного впливу виробництва повинна вирішуватися самим підприємством з використанням сучасних методів очищення газоповітряних викидів і стічних вод, що утворюються.

Якщо говорити коротко, завдання полягає в тому, щоб уникнути подій та нещасних випадків на хімічному виробництві у пілотному чи промисловому масштабі. Як правило, нові продукти доводиться розробляти в стислий термін, оперуючи невеликою кількістю матеріалу та в екстремальних умовах. З роками кількість хімічних процесів зростає, виробництво ускладнюється, хімічні реакції стають все більш нестандартними та токсичними, а робочі умови більш небезпечними. З цієї причини, а також через ряд подій контролюючі органи та

суспільство стали суворо ставитися до регулювання. Компанії були змушені підвищити загальну безпеку хімічних процесів і розробляти більш безпечні технологічні процеси для хімічного виробництва. Якщо безпека процесу врахована ще етапі розробки, його схема дозволяє запобігти виникненню хімічних небезпек, а чи не намагатися їх нейтралізувати.

Використання сучасних комп'ютерних технологій дозволяє забезпечити безпеку виробництва у всіх умовах.

Захист периметра є першою лінією захисту безпеки будь-якого об'єкта. Засоби, що використовуються для охорони периметра, можуть змінюватись від намальованої на землі білої лінії, до складних рішень високого рівня, що включають кілька фізичних бар'єрів з численними технічними системами виявлення, безперервним спостереженням та постійним патрулюванням.

Захист периметра один із найважливіших елементів комплексу безпеки. Особливо для таких об'єктів як атомні та теплові електростанції, нафтогазопереробні підприємства, нафтові термінали, аеропорти, склади готової продукції, військові арсенали. Такі об'єкти належать до вищої категорії небезпеки та обладнуються відповідно до вимог.

# 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

Полімери, великотоннажна нафтохімія, базові промислові хімічні продукти, неорганічні хімікати та мінеральні добрива складають базові хімікати. Основним застосуванням пластику є житлове будівництво, упаковка, виробництво труб, контейнерів, різноманітних транспортних засобів, дитячих іграшок та ігор. Серед полімерів найбільше застосування має поліетилен, який використовується під час виробництва упаковки, тари, контейнерів та труб, плівки, технічних волокон. Ще одним важливим полімером є полівінілхлорид, що знаходить застосування у виробництві оздоблювальних та теплоізоляційних матеріалів, будівельних труб. Поліпропілен також використовується при виробництві тканинних та килимових покриттів. Полістирол знаходить застосування у виробництві деталей автомобілів, іграшок, радіопромисловості. Важливим матеріалом для виробництва полімерів служать продукти великотоннажної нафтохімії та супутні хімікати, що виробляються зі скрапленого попутного газу, природного газу та сирої нафти. До великотоннажних хімікатів відносять пропілен, етилен, толуол, бензол, мономерний вінілхлорид, метанол, бутадієн, стирол та ін. Дані хімікати використовуються при виробництві більшої частини полімерів та інших органічних хімікатів, а також спеціальних видів хімічних продуктів. Базовими хімічними продуктами часто є неорганічні хімікати. До них відносяться каустична сода, хлор, сіль, різні кислоти (азотна, фосфорна, соляна). Мінеральні добрива – менш значущий сегмент базових хімікатів. Вони включають азотні, фосфорні і калійні добрива. Вони використовуються у сільському господарстві. До хімічних продуктів життєзабезпечення відносять фармацевтичні препарати, біологічні субстанції, ветеринарні та діагностичні препарати, вітаміни, що активно використовуються для лікування та підтримки здоров'я людей та тварин. Спеціальні хімікати включають продукти з відносно високою доданою вартістю

і є інноваційним сегментом, що досить швидко розвивається. Ці товари цінуються над ринком через їх особливі функціональні якості. До них відносяться промислові гази, електронні хімікати (призначені для електронних приладів та обладнання), клеї, промислові хімікати, що чистять, різні захисні покриття, каталізатори. Споживчі хімікати є миючі засоби та косметику, мила, без яких ми не можемо обійтися в повсякденному житті. Таким чином, продукція хімічної промисловості широко використовується для різноманітних споживчих товарів, а також і в інших галузях економіки: будівництво, сільське господарство, обробна промисловість і сфера послуг [3]. Хімічна промисловість сама споживає близько чверті свого виробництва хімікатів. Серед головних споживачів її продукції - текстильна та автомобільна промисловість, металургія, виробництво одягу та ін.

### 1.1 Галузь застосування комп'ютерної охоронної системи

Хімічна промисловість робить основний внесок у переробку сировини у продукти, які ми використовуємо щодня. Сільське господарство, харчова промисловість, фармацевтика та засоби гігієни — це лише деякі з областей, які безпосередньо залежать від хімічної промисловості. З використанням технічних інновацій хімічні процеси постійно удосконалюються, а це означає, що їхня ефективність з точки зору енергоспоживання, тривалості та скорочення відходів також збільшується.

Незважаючи на численні досягнення, досі трапляються помилки та нещасні випадки, що мають катастрофічні наслідки для працівників хімічних підприємств та навколишнього середовища. Ось деякі з найпоширеніших причин:

1. Збій виробничої системи

Будь то людська помилка або помилка технічного обладнання, аварії, пов'язані з відмовою виробничої системи, є загрозою, яку повинні враховувати виробники хімічних речовин.

2. Стихійні лиха

Залежно від географічного положення хімічні підприємства можуть зазнавати різних стихійних лих. Наприклад, повені та землетруси можуть поставити під загрозу структурну цілісність хімічного заводу. Вони можуть спричинити витік токсичних хімічних речовин, вибухи та інші катастрофічні події.

3. Несправності систем поводження з небезпечними відходами

Через свої виробничі процеси багато хімічних заводів виробляють небезпечні відходи, з якими необхідно поводитися належним чином. Коли системи управління відходами не працюють належним чином, можуть виникнути екологічні проблеми, які торкаються всіх у цьому середовищі.

4. Теракти

Хімічні підприємства часто працюють із хімічними речовинами високого ризику. Якщо вони потраплять не в ті руки, це може спричинити серйозні наслідки. У таких вкрай невизначених умовах керівництво хімічної промисловості розробило безліч рішень, що дозволяють протистояти вищезазначеним небезпекам.

1. Виключення або заміна високонебезпечних речовин

Ризик повністю усувається, коли небезпечна речовина виключається з виробничого процесу або замінюється безпечнішою сировиною, яка може бути тієї ж мети.

2. Зміна виробничого об'єкта

Фізична реструктуризація виробничої системи іноді може повністю запобігти безпосередньому контакту робітників з небезпечною речовиною і, таким чином, фактично усунути людський фактор.

3. Захисне спорядження

Протигази, захисний одяг, рукавички та захисні окуляри захищають робітників від небезпечних матеріалів, з якими вони контактують у робочому середовищі.

4. Впровадження системи безпеки

Прості протоколи та процеси інструктують працівників про те, як реагувати у надзвичайній ситуації, та усувають будь-яку невизначеність чи плутанину, які можуть виникнути у стресовій ситуації.

Крім того, у багатьох країнах діють закони, які зобов'язують хімічні підприємства, що працюють з небезпечними речовинами, використовувати систему, яка попереджає всіх усередині підприємства та поблизу нього про будь-яку можливу небезпеку, яка може виникнути [2,3].

Для правильної роботи перерахованих вище систем необхідно встановити обладнання для контролю всіх найважливіших процесів виробництва. Потім отримані дані надіслати безпосередньо відповідальній особі центр управління, або системи попередження автоматично активуються для мінімізації ризиків.

Рисунок 1.1 – Сучасне хімічне виробництво

## 1.2 Характеристика і структура об’єкта впровадження

Товариство з Обмеженою Відповідальністю «Оптиматех» - це велике підприємство, що відноситься до хімічної галузі. Як показано на рисунку територія підприємства займає велику площу, по периметру підприємство має розміри приблизно 1 на 3 км. На показаній площі розташовані як основні виробничі потужності так і площі де розташовані склади сировини та готової продукції, допоміжні підрозділи.

Рисунок 1.2 – План схема підприємства «Оптиматех»

### 1.2.1 Структура і інформаційні особливості системи

Хімічні підприємства з позиції системного аналізу зазвичай представляють як ієрархічної структури з чотирма основними рівнями.

Перший, низький ступінь ієрархічної структури хімічного підприємства утворюють типові хіміко-технологічні процеси (ХТП).

Типові ХТП, які у апараті певного класу, є типовими об'єктами управління, котрим розроблені відповідні автоматичні системи регулювання (АСР) і управління (САУ).

Основу другого ступеня ієрархії хімічного підприємства складають агрегати, комплекси відділення, лінії, які часто називаються узагальнено хіміко-технологічними системами (ХТЗ) або складними ХТЗ.

Під хіміко-технологічною системою (ХТС) розуміють сукупність взаємозалежних технологічними потоками і діючих як одне ціле апаратів, у яких здійснюється певна послідовність технологічних операцій із переробки вихідної сировини цільові продукти.

Відмінною особливістю другого ступеня ієрархії хімічних виробництв є поєднання енергетичних та хімічних вузлів у єдину енерготехнологічну систему, що здійснює рекуперацію хімічної енергії.

Третім щаблем ієрархічної структури хімічного підприємства є виробничі процеси, які можна як сукупність складних хіміко-технологічних систем.

Хімічне підприємство в цілому є четвертим, найвищим ступенем ієрархічної структури, що включає безліч виробничих процесів.


Рисунок 1.3 – Організаційна структура підприємства «Оптиматех»

## 1.3 Функціональні особливості компютерної системи охорони периметра

Досить складний алгоритм функціонування сучасного високотехнологічного виробничого підприємства можна відобразити у вигляді спрощеної структурної схеми. На структурній схемі показані основні модулі інформаційної системи, що виділяються у структурі.

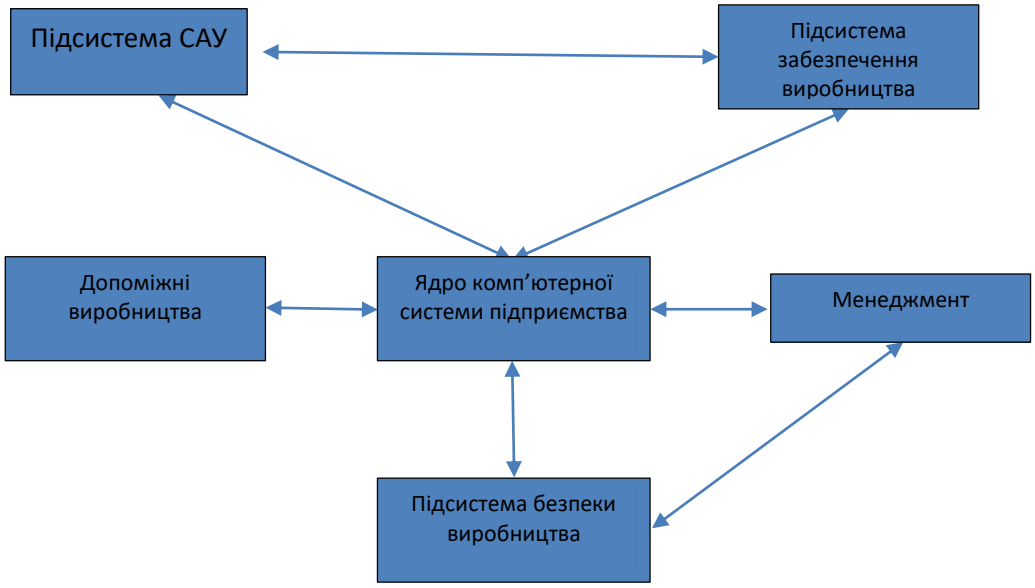


Рисунок 1.4 – Структура інформаційної системи

Система, що забезпечує охорону периметра підприємства є складовою Підсистеми безпеки виробництва в цілому.

Основні функції системи охорони периметра.

***Фізичний захист***

У народі паркан або огорожу ускладнюють і уповільнюють проникнення порушника на територію.

• Запобіжні огорожі

• Огородження з металевої сітки

• Огородження зварного типу

• Монолітні стаціонарні огорожі

***Технічні засоби***

Забезпечують раннє виявлення, локалізацію місця та напрями порушення захисту периметра. Ми докладно розглянемо технічні засоби, що найчастіше використовуються.

Системи відеонагляду

Тепловізійні системи

Радарні системи

Лідарні системи

Радіопроменеві системи

Інфрачервоні системи

Віброчутливі системи

Оптоволоконні

Трибоелектричні

Акселерометри

Провіднохвильові системи

Ємнісні системи

Магнітометричні системи

Сейсмоакустичні системи

Електрошокові системи

Рисунок 1.5 - Приклад охоронного периметру

Однак для того, щоб його ефективно використовувати, потрібно оцінити об'єкт, визначити основні загрози і розробити оптимальну стратегію захисту.

***Виявлення проникнення***

Складне, експертне завдання, але все ж таки більшість якісних систем захисту периметра її можуть вирішити, а інакше хто взагалі їх би купував. За десятки років радянськими та російськими розробниками накопичено досить серйозний досвід виявлення проникнень на будь-яких ділянках місцевості, від умов міста до водойм та периметрів у лісових умовах.

Іноземними виробниками накопичений не менший досвід, і на відміну від російського обладнання вони дорожчі, більш user friendly, а що найголовніше вони мають великі інтеграційні можливості.

Відстеження розташування зловмисника - ключ до успішного захисту периметра

Одна з найскладніших завдань, більшість систем можуть її вирішити лише приблизно, іноді це може обчислюватися сотнями метрів.

І це тому, що становище зловмисника не статично, а динамічно, тобто. він постійно пересувається, і завдання сучасних систем безпеки стежити його переміщеннями. Завдання відстеження ускладнюється ще й тим, що зловмисників може бути кілька, а це означає, що в режимі реального часу нам потрібно буде відстежувати кілька об'єктів.

Запобігання

Сенс всього захисту периметра — зупинити зловмисника, не спіймати, а саме змусити відмовитися від своїх злочинних планів. Для цього не обов'язково з автоматом навперейми бігти оглядати весь периметр. І навіть навпаки підключення охоронців це крайній захід, який несе ризики для їхнього життя та здоров'я, а отже має застосовуватися, коли всі інші заходи себе вичерпали.

Тривожна звукова сигналізація (сирена)

Голосовий зв'язок

Світлове сповіщення

Стеження за зловмисником за допомогою дрона

Висунення групи охорони до місця спрацювання сигналізації

Виклик правоохоронних органів

У практиці сучасного захисту одним із найефективніших заходів будуть голосові попередження. Голосові повідомлення можуть вимовлятись живою людиною в режимі реального часу. Як правило, досить просто повідомити зловмисника, що його виявлено, і що правоохоронні органи вже сповіщені та виїхали для його затримання. У 99% випадків, за даними моніторингової компанії Farsight, такий тиск змушує злочинця відмовитися від його планів. Але повідомлення можуть бути заздалегідь записаними, і просто програватися при спрацьовуванні охоронної сигналізації.

Звукові оповіщення почують зловмисники на об'єкті через гучномовець, але вимовляються вони операторами служби безпеки, що знаходяться на об'єкті (класика) або поза об'єктом, у віддаленому моніторинговому центрі (дивний новий світ) [1].

Фізичний захист периметра

Паркани, хоч і є низькотехнологічними пристроями, але потрапили в наш огляд, оскільки є першою лінією хорошого захисту периметра. Небагато елементів фізичної безпеки так ефективно стримують зловмисників, як захисні огородження. І до цього дня огородження забезпечують безпеку об'єктів, що найбільш захищаються.

Тип паркану часто накладає деякі обмеження на вибір технічних засобів для його охорони. Які краще розуміти ще до встановлення огорожі.

В ідеалі спочатку має бути розроблена стратегія захисту периметра, і вже відповідно до неї мають вибирати засоби захисту. У тому числі це стосується й огорожі.

Тепер подивимося на різноманітність елементів фізичного захисту периметра (або просто – огорож).

Ми розділили їх на чотири групи:

Запобіжні огорожі

Огородження з металевої сітки

Огородження зварного типу

Монолітні стаціонарні огорожі

### 1.4 Завдання і мета роботи

Завданням кваліфікаційної роботи є розробка завдання на проектування компютерної системи охорони периметру хімічного підприємства, вибір технічних засобів для реалізації системи, а також розробку корпоративної компютерної мережі підприємства.

Компютерна мережа повинна мати характеристики, які дозволяють забезпечувати ефективну роботу як системи охорони периметру так і інших систем та підсистем підприємства.

Використовувані в системі технічні засоби повинні відповідати вимогам та мати дозвіл для використання в Україні.

# 2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

## 2.1 Технічні вимоги до комп'ютерної системи

### 2.1.1 Вимоги до системи в цілому

#### 2.1.1.1 Структура і функціонування системи

Об'єкт є територією, розташованої в безпосередній близькості до населеного пункту. Підприємство розташоване на ділянці розмірами 750х1500 метрів.

На території знаходяться окремі виробничі будівлі.

На ділянці виконані ландшафтні роботи та є посадки — кущі та дерева.

Огорожа периметра

Територія оточена огорожею із 4-х сторін.

Тильна частина огорожі (зона периметра 1, довжина 1500 м) межує з лісовим масивом. Огорожа має каркасну раму з обшивкою сіткою рабиця. Висота огорожі до 2,5 м-коду.

Дві бічні частини огорожі (зони охорони 2 та 3, довжиною по 750 м кожна) межують із сусідніми ділянками. Огорожа на цих ділянках є огорожею на стрічковому фундаменті, з цегляними стовпами, з суцільною решетуванням дерев'яними дошками, висота 2,5 м.

Фасадну частину периметра (зона 4, довжиною 1500 м) звернена до дороги. Ця частина периметра є огорожею на стрічковому фундаменті, з цегляними стовпами, з суцільною решетуванням металевими конструкціями, висотою 2,5 м.

Ворота

На фасадній частині огорожі (зона 4) є двостулкові розстібні ворота та окремий пропускний пункт. Ворота та пропускний пункт у зоні 4 виконані з металевих зварних елементів, з суцільною решетуванням.

На тильній ділянці огорожі (зона 1) є хвіртка (металевий каркас з обшивкою сіткою рабиця).

Інженерна підготовка лінії периметра виконана.

Модель порушника

Найбільш важливими зонами захисту є зовнішня огорожа периметра, вхід та в'їзд на територію.

Передбачуваний порушник може мати на меті розкрадання, псування майна, терористичний акт.

Передбачуваний порушник може бути лише зовнішнім.

Система повинна виявляти порушника, що перетинає зовнішню лінію огорожі периметра різними способами -перелазом, а також за допомогою руйнування огорожі, воріт або хвірток (проломи, перепилювання або ін. механічних впливів).

Охоронні пристрої на периметрі повинні забезпечувати видачу спеціальних сигналів («Видалення») при відмови обладнання, а також при спробах розкрити або відключити датчики, встановлені на периметрі.

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

Режим роботи системи – цілодобовий.

Обслуговування системи проводиться спеціально підготованим персоналом.

Інженер з обслуговування – 4 особи.

Інженер програміст – 2 особи.

Ремонт та обслуговування обладнання виконується представниками підприємств, що виготовили це обладнання.

Для забезпечення безпеки підприємства периметр забезпечений охороною: 20 охоронців що працюють в 3 зміни. Для забезпечення швидкого доступу до зони проникнення передбачено 2 приміщення охорони, які розташовані в зонах 2,3.

Структура компютерної мережі повинна складатися з 4 локальних мереж LAN1 – LAN4.

Кількість вузлів: LAN1 – 75  LAN2 – 42  LAN3 – 16  LAN4 – 12.

Інтенсивність трафіку $\mu$ = 161 (кадрів/с).

Блок адрес - 192.168.IPn.0/24; для виділення підмереж IPn = 16.

Зовнішня адреса HTTP-сервера: 209.165.200.4.

Середня довжина вихідного повідомлення в мережі – 650 байт.

Затримка передачі пакету в найбільшій мережі  – ≤6 мс.

**2.1.1.3 Вимоги до надійності**

Значення надійності системи охорони. Для сучасних систем, ймовірність виявлення має бути близько 98% і коливатися залежно від умов експлуатації.

Визначити допустиму частоту помилкових спрацьовувань. Це показник, який показує кількість тривожних спрацьовувань без реальної загрози. Для сучасних систем цей показник не перевищує 1 спрацьовування за 10 діб роботи на периметрі довжиною 250 метрів.

Проаналізувати можливі уразливості системи захисту. Вразливість системи захисту – це можливість «зламати» подолати периметр не викликавши сигналу тривоги.

При виборі системи захисту виходити з принципу оптимальності співвідношення ціна-якість [13].

**2.1.1.4 Вимоги безпеки**

СОП має забезпечувати:

• незалежну дистанційну постановку та зняття з охорони ділянок периметра з чергового посту з видачею сигналу тривоги у разі несанкціонованого

проникнення на територію об'єкта або несанкціонованого розтину блоків та/або пошкодження сигнальних шлейфів;

• цілодобовий контроль периметра об'єкта;

• видачу оперативної інформації на робочий пульт центрального поста та дисплей комп'ютера підтримки;

• ведення протоколу подій у пам'яті комп'ютера та у пам'яті охоронного центру;

• відображення на екрані монітора комп'ютера відомостей про сигнал «Тривога» з прив'язкою до плану об'єкта або його частини.

- Google Chrome версії 28 та вище.

### 2.1.1.5 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.

Вимоги до способів та засобів зв'язку для інформаційного обміну між компонентами систем передбачити згідно з документацією виробників систем, а також протоколом випробувань, підготовленим у ході реалізації робіт.

### 2.1.1.6 Вимоги до захисту від несанкціонованого доступу

Потрібно оцінити можливі слабкі місця об'єкта, які зловмисник може використати для проникнення та використовувати цю інформацію для посилення контролю у цих зонах та запобігання розвитку негативних сценаріїв.

• Рух у мертвих зонах системи відеоспостереження, особливе значення у цьому випадку має ескізний проект, який дозволяє уникнути мертвих зон на

стадії проектування;

• Псування кабелю або контролерів системи захисту периметра;

• Імітація кількох тривог поспіль, щоб змусити охорону відключити конкретну ділянку периметра (особливо у вихідний або вночі);

• Проникнення в зонах воріт або хвірток як менш захищених ділянках периметра;

• Перестрибування/перелаз огорожі, сюди ж віднесемо перекидання предметів через огорожу, якщо зловмисник діє зсередини;

• Здійснення підкопу під огорожу;

• Характеристики охоронного освітлення, низька якість якого часто є критичним чинником своєчасного виявлення зловмисника.

#### 2.1.1.7 Вимоги до патентної чистоти

Відповідальність за дотримання патентного законодавства лежить на розробниках проекту системи охорони периметра.

#### 2.1.1.8 Вимоги до стандартизації й уніфікації

У систему сигналізації охорони периметра орієнтовно має входити таке основне обладнання:

• датчики виявлення перетину зовнішнього периметра;

• датчики виявлення перетину людиною верхньої частини воріт та даху прохідного.

Кількість зон охорони периметра визначається виконавцем і відповідає типу та стану огорожі.

Устаткування має бути уніфіковано.

### 2.1.2 Вимоги до видів забезпечення

#### 2.1.2.1 Інформаційне забезпечення системи

СОП має забезпечувати:

• незалежну дистанційну постановку та зняття з охорони ділянок периметра з чергового посту з видачею сигналу тривоги у разі несанкціонованого проникнення на територію об'єкта або несанкціонованого розтину блоків та/або пошкодження сигнальних шлейфів;

• цілодобовий контроль периметра об'єкта;

• видачу оперативної інформації на робочий пульт центрального поста та дисплей комп'ютера підтримки;

• ведення протоколу подій у пам'яті комп'ютера та у пам'яті охоронного центру;

• відображення на екрані монітора комп'ютера відомостей про сигнал «Тривога» з прив'язкою до плану об'єкта або його частини.

• Оперативний контроль дій співробітників служби безпеки (підрозділу охорони) та надання необхідної інформації для координації цих дій;

• Запис відеоінформації в архів для подальшого аналізу стану об'єкта, що охороняється, тривожних ситуацій, ідентифікації порушників;

• Взаємодія з іншими підсистемами інтегрованої системи безпеки забезпечення протикримінального захисту з метою забезпечення протикримінального захисту об'єкта, що охороняється;

• Взаємодія з системою збору результатів технічного моніторингу та контролю при отриманні та передачі інформації у вказану систему через локальну мережу Ethernet з використанням стека протоколів сімейства TCP/IP;

• Обмін інформацією із системою збору результатів технічного моніторингу та контролю з використанням уніфікованих протоколів передачі даних та формату метаданих, розробленого на основі XML.

AXIS Perimeter Defender — це масштабована аналітична програма, яку

можна встановити на будь-яку необхідну кількість мережевих камер. Працює безпосередньо в мережевій камері та аналізує відео на наявність тривожних подій. Оскільки відео не передається для аналізу на центральний сервер, немає необхідності в установці додаткового обладнання. Роблячи систему гнучкою і масштабованою, додаток, крім того, знижує обсяг трафіку, що передається в мережі, і вимоги до обсягу пам'яті для зберігання даних.

#### 2.1.2.2 Технічне забезпечення системи

Огородження зварного типу.

Більш надійні металеві огорожі - це огорожі зварного типу, що використовують сталевий профіль більшого перерізу, ніж рабиця, яка не вільно переплетена, як сітка, а надійно зварена між собою.

Однак і цей вид огорож схильний до механічного пошкодження, хай не ручним способом, але із застосуванням спецтехніки зловмисники зможуть його без проблем перерізати.

Крім цього зварна огорожа не перешкоджає перегляду території як людиною, так і камерами відеоспостереження. Це саме собою сприяє зниженню кількості злочинів. Адже ви пам'ятаєте, що природне спостереження це одна з концепцій CPTED. Потенційні порушники відчувають підвищену увагу себе і, таким чином, відчувають збільшення ризику необхідного скоєння злочину.

Але найголовніше в тому, що через дрібний розмір осередку, дуже важко закріпитися на цій огорожі, а ріжучі інструменти, необхідні для розрізання важкого сталевого дроту, не завжди зможуть поміститися в мінімальному просторі сітки.

Технічні засоби, які можна використовувати лише з огорожею:

Віброчутливі системи

Оптоволоконні

Трибоелектричні

Акселерометри

Провіднохвильові системи

Ємнісні системи

Електрошокові системи

Оптоволоконні

Оптоволоконна система захисту периметра.

Як сенсорний кабель використовують оптоволокно, яке має бути змонтоване на огорожі. При найменшій деформації кабелю змінюється довжина хвилі світлового променя, що у кабелі. Приймальний прилад реєструє ці зміни та в залежності від налаштування видає тривогу. Спочатку оптоволоконні системи були системами зонального типу з урахуванням многомодового волокна. Вони показали свою ефективність, але мали кілька недоліків. Кожен відрізок волокна був одним датчиком, таким чином, периметр, що охороняється, ділився на зони 100-250 метрів, на які розварюється потрібне число волокон. Відповідно визначити місце дії можна було лише з точністю до ста метрів, також необхідно було проводити варіння волокон на периметрі. Цей клас систем економічно вигідно використовувати на протяжних периметрах 2 км і більше.

Існують контролери, які вимагають установки на огорожі, але є й такі, які можуть бути встановлені на відстані до 20 км. від периметра, тобто. на самому огорожі розташовуватиметься тільки оптоволоконний провід, який можна приховати.

Оптоволоконні системи можуть використовуватися в умовах вибухо- або пожежонебезпечних середовищ, оскільки в чутливому кабелі, що розташовується безпосередньо по периметру, поширюється тільки світловий сигнал, а всі електричні і струмопровідні частини можуть бути винесені за межі небезпечної зони. Оптоволоконний кабель також нечутливий до Електромагнітне випромінювання, такі системи можна використовувати поряд з ЛЕП або на електропідстанціях [1,14].

Відеоспостереження для захисту периметра

Ефективного захисту периметра без системи відеоспостереження не може бути в принципі.

Верифікувати помилкові спрацьовування можна лише за допомогою системи відеоспостереження. Іншого гарного рішення немає.

Однак, верифікацією подій справа не обмежується, відеоспостереження може принести значно більше користі.

Однією своєю наявністю відеоспостереження знижує рівень крадіжок на 14%, про це повідомляє систематичний огляд, в якому проводився мета-аналіз 76 досліджень.

Система охоронного відеоспостереження за периметром забезпечує:

• Відеоверифікацію тривог (підтвердження за допомогою відеоспостереження факту несанкціонованого проникнення в зону охорони та/або виявлення хибних спрацьовувань);

• Візуальний контроль об'єктів охорони та прилеглих до них територій (пряме відеоспостереження);

### 2.1.2.3 Вимоги до організаційного забезпечення

Обчислювальний центр. Під ним мається на увазі електронний блок управління - комп'ютер, який отримує сигнали від сенсорів та датчиків. Саме ця електронно-обчислювальна машина в сучасних системах включає сирену, активує ту чи іншу камеру або підсвічування. Крім того, електронний блок активує різні пасивні режими захисту, а також надсилає сигнал озброєній охороні.

Особи служби охорони підприємства набувають відповідного статусу з моменту видання наказу про призначення на відповідну посаду у приватному охоронному підприємстві та наказу про заступлення на службу з охорони підприємства.

Кожен співробітник служби охорони зобов'язаний:

знати організацію та зміст діяльності приватного охоронного підприємства;

знати свої посадові обов'язки та права, а також обов'язки та права на щабель вище займаної посади;

суворо дотримуватись вимог, що пред'являються до приватних охоронців, зберігати в таємниці інформацію про підприємства, що стала їм відомою під час виконання охоронних функцій;

досконало володіти засобами охорони підприємства;

постійно вдосконалювати свою спеціальну та фізичну підготовку;

бути дисциплінованим, вміти володіти собою у складних ситуаціях, правильно та швидко приймати рішення діяти самостійно, ініціативно, сміливо та рішуче, бути чуйним та чуйним до людей;

володіти загальною обстановкою в регіоні та в оточенні підприємства, що охороняється (об'єкта);

знати місця знаходження місцевих правоохоронних органів, інших охоронних структур та підтримувати з ними ділові відносини [16].

#### 2.2.1.4 Вимоги до складу нормативно-технічної документації системи

Інформація про склад та характеристику системи охорони периметра, план розташування датчиків, відеоспостереження є інформацією з обмеженим доступом.

Технічна документація має бути представлена в двох екземплярах. Між замовником та розробником підписується додаткова угода про нерозповсюдження інформації про проект.

## 2.2 Структура системи охорони периметра

Система охорони периметра складається з однотипних по складу ділянок. Довжина кожної ділянки – 500 метрів (Рис. 2.1).

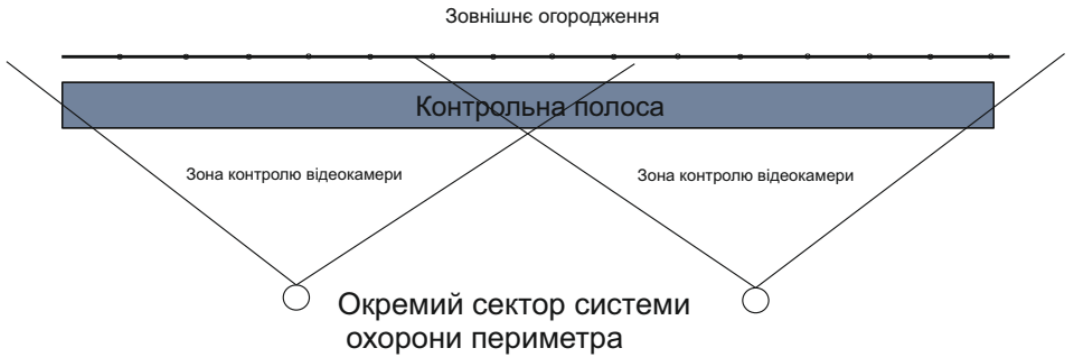


Рисунок 2.1 – Схема ділянки системи охорони периметра.

На схемі показана огорожа, за огорожею реалізована контрольна полоса.

За 20-30 м від огорожі встановлено стовпи на яких розташовані відеокамери. Зони контролю відеокамер перехрещуються.

В цілому охоронний периметр схематично показаний на рисунку 2.2.

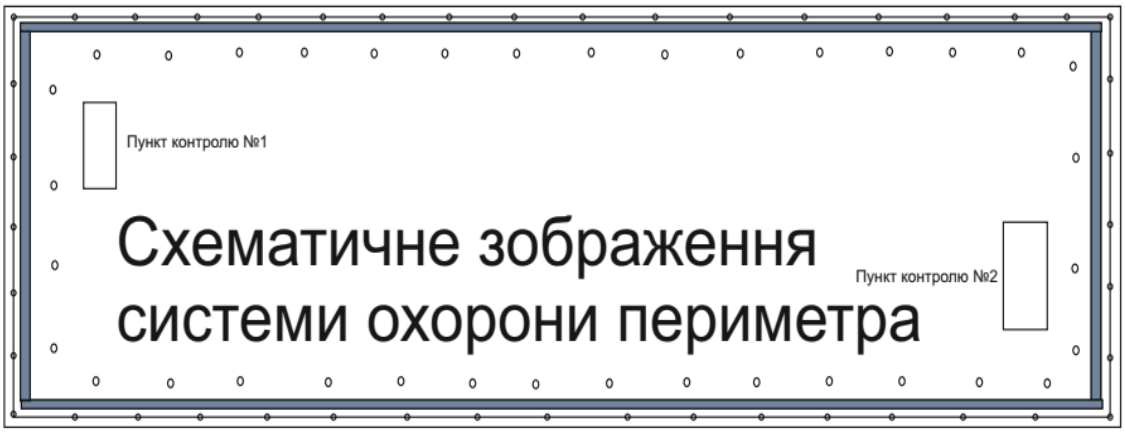


Рисунок 2.2 – Схема системи охорони периметра

На схемі показано практично ті ж елементи як і на рис.2.1. Також показано 2 пункти, в яких розташовано приміщення для охоронців та обслуговуючого персоналу.

### 2.3 Розробка структурної схеми комп’ютерної системи

На розробленій структурній схемі компютерної мережі показано усі елементи компютерної системи, на цій схемі показано окрему локальну мережу, що виділена для роботи системи охорони периметру.

LAN1 – 75

LAN2 – 42

LAN3 – 16

LAN 4 – 12

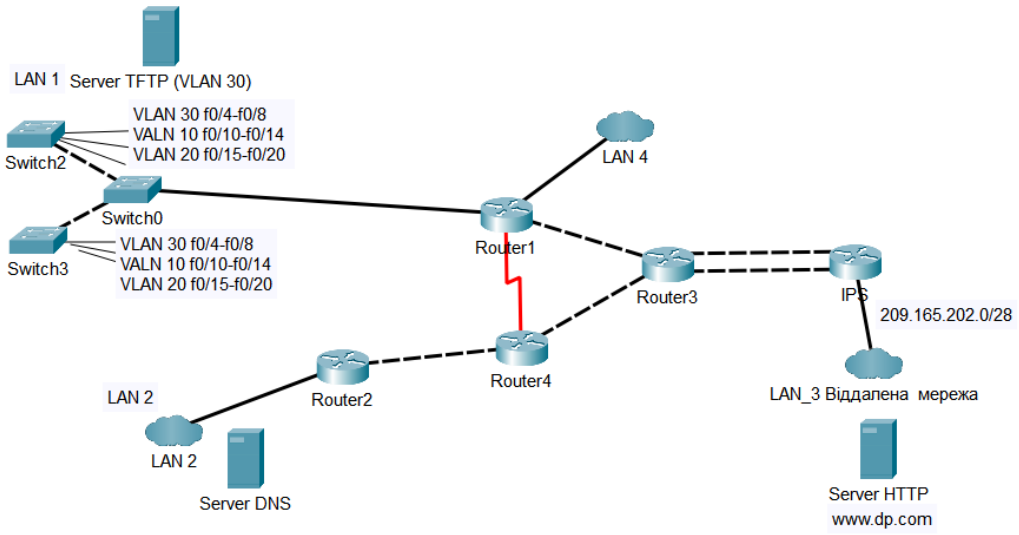


Рисунок 2.3 – Структура комп’ютерної мережі підприємства

## 2.4 Характеристика технічних пристроїв що складають комп’ютерну мережу

Оптоволокно

Найбільш важливими перевагами оптоволокна є: імунітет до електромагнітних перешкод, безпека передачі інформації, висока пропускна спроможність та можливість передачі на значні відстані без необхідності проміжного посилення. Крім цього можна заощадити на грозозахисті, адже оптоволоконний кабель складається з діелектрика.

Це не дешево, але як бонус, ви можете використовувати прокладену лінію і для охорони як віброзахист.

Переваги

• Висока чутливість оптоволоконного кабелю до вібрацій

• Застосування оптики можливе не тільки на огорожі, подібні системи можуть монтуватися на невеликій глибині і реагувати на переміщення людей або техніки в зоні, що охороняється.

• Можливий прихований монтаж

• На оптоволоконний кабель не впливають погодні умови та електромагнітне випромінювання, можливе використання в небезпечних середовищах (вибухо- пожежонебезпечні території)

• Не потрібний монтаж контролерів-аналізаторів на огорожі

• Один аналізатор може обробляти до 5 км (а деякі й більше) периметра.

• Можна використовувати оптоволоконну лінію системи відеоспостереження

Недоліки

• Дорогі контролери

• Дорогий кабель

• Вимагають кваліфікації персоналу для налаштування та обслуговування

• Підходять не для всіх огорож. Потрібно відповідально підійти до вибору огорожі, щоб виключити помилкові тривоги, пов'язані з коливанням самої огорожі в ситуаціях, які не пов'язані зі спробами проникнення (погодні умови, сейсмо-умови тощо), наприклад, не підходить для рабиці [18,19].

Аналізатор Optex Fiber Sensys FD-342, 2 зони

Аналізатори серії FD-34x підтримують можливість підключення 5000 м сенсорного кабелю для захисту протяжних ділянок периметра (довжина зони до 2 км).

Самі аналізатори можуть бути встановлені при цьому в контрольному центрі на відстані до 20 км від зони, що охороняється, підключення сенсорного кабелю проводиться за допомогою стандартного одномодового оптоволокна.

При використанні такої конфігурації відпадає необхідність підведення додаткових проводів живлення та сигнальних проводів безпосередньо до периметра. Це дозволяє суттєво спростити систему, повністю виключивши прокладання мідних кабелів на периметрі.

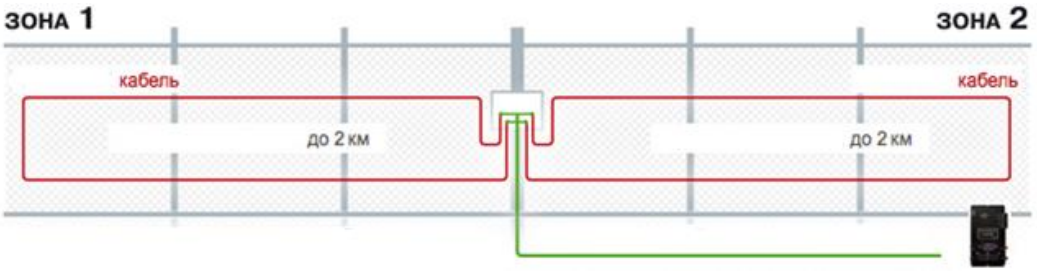


Рисунок 2.4 – Секція периметра

| | |
|---|---|
| Бренд | Optex |
| Вид обладнання | Аналізатор |
| Охоронні зони | 2 |
| Довжина охоронної зони, м | 2000 |
| Напруга живлення | 12 В / 24 В |
| Потужність, макс. | 3 Вт |
| Робоча температура | от -40°C до +70°C |
| Гарантія | 2 роки |
| Країна виробництва | Японія |

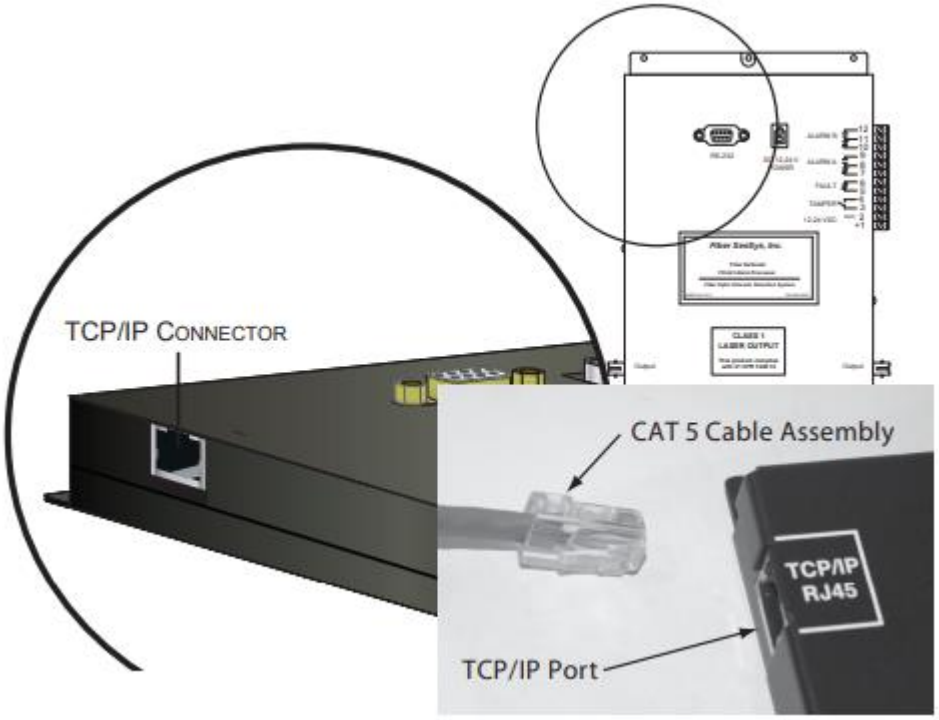


Рисунок 2.5 – Контролер секції периметра, можливі підключення

IP-камера PTZ-Y2404I-DE (2.8-12 мм) є 4 Мп циліндричною IP-камерою з функцією «поворот + нахил» та варіофокальним об'єктивом.

Особливості:

• Висока якість зображення з роздільною здатністю 4 Мп

• Можливість повороту, нахилу та зуму для більшого огляду та захоплення областей інтересу

• Захист від вологи та пилу: IP66

• EXIR 2.0: покращена інфрачервона технологія з великою дальністю ІЧ-підсвічування

• Технологія ефективного стиснення H.265+

• Вбудований слот для microSD/SDHC/SDXC: є, до 256 ГБ

• Вбудований мікрофон: є

Підсвічування EXIR 2.0 – інноваційне рішення для якісної нічної зйомки.

EXIR 2.0 є розширенням технології EXIR 1.0 і не тільки успадковує її переваги, такі як тонкоплівкове світловипромінювання, високу світлову віддачу, низький тепловий опір та тривалий термін служби, але й набуває нових особливостей, що перевершують EXIR 1.0 та DIP ІЧ-світлодіоди. Все це сприятиме тому, що ви отримаєте дійсно якісне зображення в нічний час, що дозволяє без проблем розглянути все, що сталося.


Рисунок 2.6 – Камера відеоспостереження

Характеристики:

Камера

• Матриця: 1/3″ Progressive Scan CMOS

• Максимальна роздільна здатність: 2560 × 1440

• Чутливість: Колір: 0.007 лк @ (F1.0, AGC вкл.), 0 лк з підсвічуванням

• Швидкість електронного затвора: від 1/3 до 1/100,000 с

• Режим «День/ніч»: ІЧ-фільтр

• Регулювання кута: поворот: від -100 до +100°, нахил: від -20 до +45°

Об'єктив

• Тип об'єктиву: Варіофокальний об'єктив, моторизований об'єктив, від 2.8 до 12 мм

• Фокусна відстань та кут огляду: від 2.8 до 12 мм, по горизонталі: від 96.7 до 29.7°, по вертикалі: від 51.7 до 16.7°, по діагоналі: від 114.3 до 34°

• Кріплення об'єктива: Ø 14

• Тип діафрагми: Фіксована

• Апертура: Макс. F1.6

DORI

• Варіофокальний об'єктив:

- Wide: D: 64 м, O: 25 м, R: 12 м, I: 6 м

- Tele: D: 200 м, O: 75 м, R: 40 м, I: 20 м

Підсвічування

• Тип підсвічування: ІЧ-підсвічування

• Дальність підсвічування: До 50 м

• Додаткове інтелектуальне підсвічування: Є

• Інфрачервоні хвилі: 850 нм

Відео

• Основний потік:

- 50 Гц: 20 к/с (2560 × 1440), 25 к/с (1920 × 1080, 1280 × 720)

- 60 Гц: 20 к/с (2560 × 1440), 30 к/с (1920 × 1080, 1280 × 720)

• Додатковий потік:

- 50 Гц: 25 к/с (1280 × 720, 640 × 480, 640 × 360)

- 60 Гц: 30 к/с (1280 × 720, 640 × 480, 640 × 360)

• Відеостиснення:

- Основний потік: H.265+/H.265/H.264+/H.264

- Додатковий потік: H.265/H.264/MJPEG

• Бітрейт відео: Від 32 Кбіт/с до 8 Мбіт/с• Профиль H.264: Baseline Profile / Main Profile / High Profile

• Профіль H.265: Main Profile

• Бітрейт: CBR/VBR

• Область інтересу (ROI): 1 фіксована область для основного потоку

Аудіо

• Тип аудіо: Моно

• Фільтрування шумів довкілля: Є

• Частота дискретизації: 8/16 кГц

• Аудіостискання: G.711ulaw / G.711alaw / G.722.1 / G.726 / MP2L2 / PCM / AAC-LC

• Бітрейт аудіо: 64 Кбіт/с (G.711 ulaw) / 64 Кбіт/с (G.711 alaw) / 16 Кбіт/с (G.722.1) /16 Кбіт/с (G.726) / від 32 до 160 Кбіт/с (MP2L2) / від 16 до 64 Кбіт/с (AAC-LC)

Мережа

• Безпека: Захист паролем, складний пароль, шифрування HTTPS, автентифікація 802.1X

(EAP-MD5), водяні знаки, фільтрація IP-адрес, базова та дайджест-автентифікація для HTTP/HTTPS, WSSE та дайджест-автентифікація для ONVIF, RTP/RTSP через HTTPS, журнал перевірки безпеки, TLS 1.2, аутент адреса)

• Одночасний перегляд у реальному часі: До 6 каналів

• API: Відкритий мережевий відеоінтерфейс (PROFILE S, PROFILE G), ISAPI, SDK

• Протоколи: TCP/IP, ICMP, DHCP, DNS, DDNS, HTTP, HTTPS, RTP, RTSP, NTP, UPnP, IGMP, IPv6, UDP, QoS, Bonjour, FTP, 802.1x, SMTP

• Користувач/хост: До 32 користувачів. 3 рівня: адміністратор, оператор та користувач

• Клієнт: iVMS-4200, Hik-Connect

• Веб-інтерфейс:

- Потрібен плагін для перегляду в режимі реального часу: IE 10, IE 11

- Локальні послуги: Chrome 57.0+, Firefox 52.0+

Зображення

• Широкий динамічний діапазон (WDR): 120 дБ WDR

• SNR: ≥ 52 дБ

• Переключення «День/ніч»: День/Ніч/Автоматич. / За розкладом

• Покращення зображення: BLC, HLC, 3D DNR

• Налаштування зображення: Дзеркало, насиченість, яскравість, контрастність, різкість, посилення та баланс білого налаштовуються через клієнтське ПЗ або веб-інтерфейс

• Маскування області: 4 області маскування

Інтерфейси

• Інтерфейс Ethernet: 1 RJ45 auto 10 / 100 M Ethernet

• Локальне зберігання - слот для карти памяті, підтримка microSD / microSDHC / microSDXC, до 256 ГБ

• Встроений мікрофон: Є

Мережа

• Безпека: Захист паролем, складний пароль, шифрування HTTPS, автентифікація 802.1X
(EAP-MD5), водяні знаки, фільтрація IP-адрес, базова та дайджест-автентифікація для HTTP/HTTPS, WSSE та дайджест-автентифікація для ONVIF, RTP/RTSP через HTTPS, журнал перевірки безпеки, TLS 1.2, аутент адреса)

• Одночасний перегляд у реальному часі: До 6 каналів

• API: Відкритий мережевий відеоінтерфейс (PROFILE S, PROFILE G), ISAPI, SDK

• Протоколи: TCP/IP, ICMP, DHCP, DNS, DDNS, HTTP, HTTPS, RTP, RTSP, NTP, UPnP, IGMP, IPv6, UDP, QoS, Bonjour, FTP, 802.1x, SMTP

• Користувач/хост: До 32 користувачів. 3 рівня: адміністратор, оператор та користувач

• Клієнт: iVMS-4200, Hik-Connect

• Веб-інтерфейс:

- Потрібен плагін для перегляду в режимі реального часу: IE 10, IE 11

- Локальні послуги: Chrome 57.0+, Firefox 52.0+

Подія

• Основні події: Виявлення руху, детектор саботажу, виключення

• Прив'язка: Завантаження на FTP / карту пам'яті, повідомлення центру моніторингу, відправка email, запис тривоги, захоплення зображення

Основне

• Живлення:

- DC 12 ± 25 %, 0.91 A, макс. 11 Вт, коаксіальний роз'єм живлення Ø 5.5 мм, захист від зворотної полярності,

- PoE: 802.3af, клас 3, від 36 до 57, від 0.34 до 0.21 A, макс. 12.5 Вт

• Матеріал: Передня частина: метал, основна частина корпусу: пластик, кронштейн: пластик

• Розміри: 197.1 × 105 × 225.4 мм (7.8 × 4.1 × 8.9″)

• Розмір упаковки: 300×266×172 мм (11.8×10.4×6.8″)

• Маса: Прибл. 900 г

• Маса з упаковкою: Прибл. 1520 г

• Умови зберігання: від -30 до +60 °C. Вологість 95% або менше (без конденсату)

• Робочі умови: від -30 до +60 °C. Вологість 95% або менше (без конденсату)

• Мова: Англійська, російська

• Основні функції: Anti-Flicker, Heartbeat, захист паролем, зміна пароля E-mail

Сертифікати

• Стандарти EMC:

- CE-EMC: EN 55032: 2015, EN 61000-3-2:2019, EN 61000-3-3: 2013+A1:2019, EN 50130-4: 2011+A1: 2014;

- RCM: AS / NZS CISPR 32: 2015,

- IC: ICES-003: Issue 7,

- KC: KN32: 2015, KN35: 2015, FCC: 47 CFR Part 15, Subpart B

• Безпека:

- UL: UL 62368-1,

- CB: IEC 62368-1: 2014 + A11,

- CE-LVD: EN 62368-1: 2014/A11: 2017,

- BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005

• Навколишнє середовище: CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006

• Захист IP66: IEC 60529-2013

Оператори відеоспостереження не можуть утримувати увагу на перегляд відео з камер, оскільки 99% часу на периметрі нічого не відбувається. Згодом охоронці перестають звертати увагу на монітори, і можливість пропуску тривожної події дуже велика.

Стандартні можливості відеоаналітики зараз присутні навіть у недорогих відеокамерах. Найчастіше для цілей охорони периметра використовується класичний детектор руху, детектор перетину лінії, детектор вторгнення в зону, детекція людини та автотранспорту.

Практично всі ці детектори можна знайти в будь-якому дешмані з Аліексперс.

Тому важлива не сама наявність відеоаналітики, а то наскільки якісно її реалізовано.

Проблема малоконтрастних об'єктів

Детектор може пропустити людину в маскувальному костюмі вдень, і людину в чорному одязі вночі. Додатково негативно впливатимуть на детекцію погодні умови, які знижують контрастність — туман, дощ, сніг.

Детектор руху не зафіксує перекидання предметів через огорожу

Якщо об'єкт, що перекидається, не дуже великий, детектор не спрацює, навіть якщо перекидання здійснюється близько від камери.

Детектор руху генерує помилкові спрацьовування

Будь-який детектор генеруватиме помилкові спрацьовування. Дощ, сніг, комаха джерело помилкових спрацювань детектор руху. Комахи особливий бич, що приваблюють тепло від камери.

XMG1930-30-ZZ0101F — Гібридний Smart L2+ комутатор Zyxel NebulaFlex XMG1930-30, rack 19″, 24xRJ-45: 1/2.5G, 4xRJ-45: 1/2.5/5/10G, 2

Серія XMG1930 - це сімейство мультигігабітних Smart L3 Lite комутаторів, що включає 2 моделі (одна з них з PoE). Вона відрізняється високою щільністю мультигігабітних портів для точок доступу Wi-Fi 6/6E, серверів та робочих станцій. Обидві моделі підтримують технологію NebulaFlex і відрізняються простотою, корисними функціями та чудовою продуктивністю.

Ідеальне рішення для модернізації вашої мережі

XMG1930 має шість аплінків 10G (мідь та оптика), які дозволяють розширювати мережу та гнучко розгортати її в будь-яких сферах використання, а також 8 портів PoE++ (60 Вт) для впровадження точок бездротового доступу Wi-Fi 6/6E та Wi-Fi 7 в найближчому майбутньому.

Різностороннє управління

Серія XMG1930 підтримує безкоштовне централізоване керування Nebula. Nebula надає як інтуїтивно зрозумілий веб-інтерфейс, так і мобільний додаток для спрощення встановлення та керування вашою мережею без додаткових витрат на програмний або апаратний контролер. Класичний автономний режим, як і раніше, доступний для використання.

Мережа на долоні з мобільним додатком

• Швидка реєстрація пристроїв за QR-кодом

• Огляд стану мережі

• Віддалене управління

• Перезавантаження PoE пристроїв шляхом скидання живлення

• Блокування клієнтів із незвичайним трафіком

Екосистема Nebula

Підтримка Zyxel Nebula дозволяє будь-коли отримати єдину централізовану мережу з комутаторів, точок доступу, міжмережевих екранів і роутерів 5G/4G.

Серія XMG1930 підтримує спеціалізований Networked AV інтерфейс під час використання в автономному режимі. Ви можете перемикати інтерфейси, щоб спростити встановлення AVoIP за допомогою інтуїтивно зрозумілого майстра, який підказує вимоги щодо налаштувань для цього типу мережної інфраструктури. Комутатор полегшує конфігурацію, використовуючи всі необхідні деталі для налаштування професійного розгортання AVoIP за лічені хвилини.

При виборі інтерфейсу Networked AV комутатор надає спеціальну панель інструментів, що забезпечує швидкий доступ до ключових елементів мережі AV, наприклад інформація про IGMP, а також швидкий доступ до функцій, пов'язаних з розгортанням AVoIP.

Потрібна додаткова ліцензія та прошивка версії 4.80 або вище.

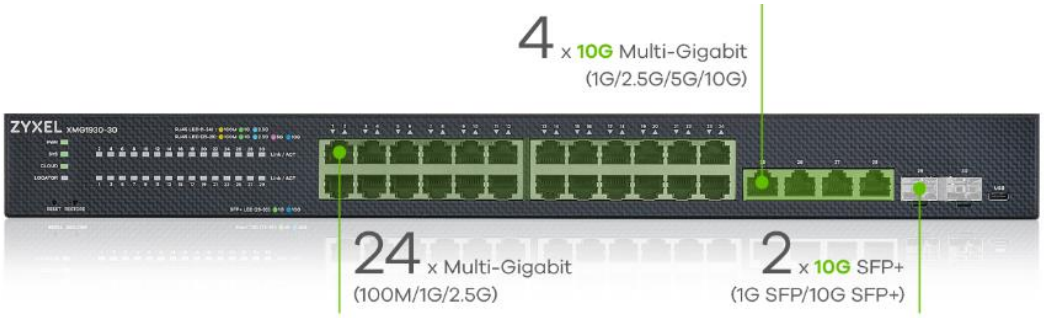


Рисунок 2.7 – Зовнішній вигляд комутатора

SA-2006/A1A — сервісний маршрутизатор D-Link, оснащений 6-ю Ethernet-портами 1 Гбіт, кожен з яких можна використовувати як LAN- або WAN-порт, 2-ма портами USB 2.0 і консольним портом з роз'ємом mini-USB . Призначений для застосування в малому та середньому бізнесі для захисту мережевої інфраструктури від зовнішніх загроз та організації безпечного підключення до VPN. Маршрутизатор підтримує одночасне підключення великої кількості користувачів. Форм-фактор пристрою передбачає його встановлення у стійку.

Спосіб управління:

• За допомогою вбудованого веб-інтерфейсу;

• Можна оновити вбудоване програмне забезпечення – маршрутизатор сам знаходить перевірену версію програмного забезпечення на сервері оновлень D Link і повідомляє користувача про готовність встановити його.

Розширені можливості маршрутизатора:

• Функція розкладу для застосування правил та налаштувань міжмережевого екрану та перезавантаження маршрутизатора у вказаний час або через задані інтервали часу;

• Підтримка роботи з сервісом контентної фільтрації SkyDNS, який пропонує більше налаштувань та можливостей для забезпечення безпечної роботи в Інтернеті.


Рисунок 2.8 – Зовнішній вигляд маршрутизатора

Функції безпеки мережі:

• Функція блокування реклами – ефективно блокує рекламні оголошення, що виникають під час перегляду веб-сторінок;

• Підтримка протоколу SSH — підвищує безпеку при віддаленому налаштуванні маршрутизатора та керуванні ним за рахунок шифрування всього трафіку, що передається, включаючи паролі;

• Підтримка безлічі типів тунелів для організації безпечного підключення VPN: IPsec (IKEv1/IKEv2), L2TP over IPsec, PPTP/L2TP, GRE, IPIP, EoGRE, а також некеровані L2TPv3-тунелі;

• Розширені функції безпеки підтримують поділ мережі на зони, налаштування політик для взаємодії зон та правил фільтрації трафіку з широким вибором параметрів.

| | |
|---|---|
| Артикул: | DSA-2006/A1A |
| Код товару: | 12587 |
| 1 Гбіт/с LAN: | 6 |
| Процесор: | Intel Atom C2358 |
| Кількість ядер процесора: | 2 |
| Частота процесора, МГц: | 1740 |
| Об'єм ОЗУ, МБ: | 2 048 |
| Тип ОЗУ: | DDR3 |
| Об'єм ПЗУ, МБ: | 4 096 |
| Тип ПЗП: | eMMC |
| USB-порти: | 2 |
| Тип USB: | USB 2.0 |
| Консольний порт: | mini-USB |

Сервер та його характеристика

2 x Intel Xeon E5-2620v4 (2.10GHz, 8C, 20MB, 8.0GT/s QPI, 85W), 128GB (8 x 16GB) Dual Rank RDIMM 2133MHz, 4 x 300GB SAS 12Gbps 15k 2.5" Hot Plug (up to 8 x 2.5"), PERC H730p RAID Controller 2GB cache, DVD+/-RW, Broadcom 5720 Quard Port 1GbE, IDRAC8 Enterprise, RPS 2 x 550W HS, Bezel, Sliding Rack Rails with arm, 1U, 3y NBD

Рисунок 2.9 – Зовнішній вигляд сервера

Таблиця 2.1 - Характеристики ПК та серверів

| Найменування | Характеристики |
|---|---|
| 1 | 2 |
| ПК 1 – ПК 75 | Материнська плата: Asus P8H77-V LE<br>Процесор: Intel core i5<br>Відео адаптер: Gigabite redeon HD6570 2048mb<br>HDD: Seagate 1000Gb 64 MB<br>DVD привод: Asus DRV-24x<br>Оперативна пам'ять: Kingston DDR-4 PC-3 8 Gb<br>Блок живлення: AeroCool VP750W<br>Корпус: Metal Master SG2<br>Монітор: Samsung PN22"<br>Клавіатура: BTC Keyboard120<br>Мишка: Logitech LTC-19 |
| ПК 76-126 | HDD: Seagate 320Gb 64 MB<br>DVD привод: Asus DRV-24x<br>Оперативна пам'ять: Kingston DDR4 PC-3 2 Gb<br>Блок живлення: AeroCool VP500W<br>Корпус: LogicPower SK789-2<br>Монітор: Samsung E1920<br>Клавіатура: BTC Keyboard120<br>Мишка: Logitech LTC-19 |
| Шлюз та Firewall | 2 процесора Intel Xeon "Multi Core";<br>чіпсет Intel i5000V, 2xPCI-E 8x, 2xPCI-X 64bit/133MHz;<br>8 GB ECC DDR4 667 FBD (4/8 DIMMs);<br>відеокарта ATI Rage Pro 16Mb onboard;<br>блок живлення 750W Fi; |
| Web- сервер | 2 x Intel Xeon E5-2620v4 (2.10GHz, 8C, 20MB, 8.0GT/s QPI, 85W), 128GB (8 x 16GB) Dual Rank RDIMM 2133MHz, 4 x 300GB SAS 12Gbps 15k 2.5" Hot Plug (up to 8 x 2.5") |
| Контролер домена | Процесор Intel C202, 1xLGA1155, RAM: 8 GB DDR3 1600MHz ECC Unbuffered, 1xHDD Seagate 320Gb SATA 3Gb/s. Intel C202 (RAID levels: 0,1,5,10), Intel graphic mode video |
| Файловий сервер | 2 x Intel Xeon E5-2620v4 (2.10GHz, 8C, 20MB, 8.0GT/s QPI, 85W), 128GB (8 x 16GB) Dual Rank RDIMM 2133MHz, 4 x 300GB SAS 12Gbps 15k 2.5" Hot Plug (up to 8 x 2.5") |
| Storage | Процесор - Intel Xeon E5-2650 (6 ядер), 2.0 ГГц Ram: 16 Гб LAN: 1 Гбіт/с / LAN (RJ-45) - 2 шт. HDD: Seagate 1000Gb-SATA Hot Plug. БП - 520 Вт |

Таблиця 2.2 - Характеристики мережевого обладнання

| Найменування | Характеристика | Кількість, шт. |
|---|---|---|
| 1 | 2 | 3 |
| DSA-2006/A1A — сервісний маршрутизатор D-Link | оснащений 6-ю Ethernet-портами 1 Гбіт, кожен з яких можна використовувати як LAN- або WAN-порт, 2-ма портами USB 2.0 і консольним портом з роз'ємом mini-USB . | 5 |
| XMG1930-30-ZZ0101F — Гібридний Smart L2+ комутатор Zyxel NebulaFlex XMG1930-30 | XMG1930 має шість аплінків 10G (мідь та оптика), які дозволяють розширювати мережу та гнучко розгортати її в будь-яких сферах використання, а також 8 портів PoE++ (60 Вт) для впровадження точок бездротового доступу Wi-Fi 6/6E та Wi-Fi 7. | 6 |
| Кабель UTP кат.5е | Довжина 7305 м;<br>4 пари;<br>оболонка FR-ПВХ (IEC 332.1);<br>діаметр провідника з ізоляцією не більше ніж 0,001 м;<br>діаметр кабелю не більше ніж 0,005 м | - |

## 2.5 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Кожна локальна мережа генерує певну кількість вихідних повідомлень, які є навантаженням відповідного маршрутизатора на рівні розподілу. В залежності від продуктивності мережевих пристроїв, каналів звязку потрібна оцінка трафіку та його характеристик.

Характеристики такі: 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 визначення описаних параметрів локальну мережу приймаємо як модель мережі масового обслуговування M/M/1.

Вимоги до найбільшої мережі (LAN1):

кількість вузлів в найбільшій мережі: 75

середня інтенсивність трафіку: μ= 161 (кадрів/с)

середня довжина повідомлення: l=650 байт;

вимоги до затримки передачі пакету – ≤6 мс.

Відповдно до кількості пристроїв в мережі на рівні розподілу обираємо роутер маршрутизатор D-Link DSA-2006/A1A. (1 шт), на рівні доступу комутатор XMG1930-30-ZZ0101F — Гібридний Smart L2+ комутатор Zyxel NebulaFlex XMG1930-30 (4 шт).

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 1000 Мбіт/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=161 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність мережі на рівні доступу припускаючи, що використовуються усі порти встановленого обладнання.

Рр.д= μ*l*n*8= 161*650*96*8= 80,4 (Мбіт/с), де

n- кількість портів в комутаторі рівня доступу (96).

Зважаючи на те, що в мережі встановлені IP відеокамери в досить значній кількості, то потрібно урахувати що кожна з камер може навантажувати мережу додатковим трафіком до 8 Мбіт/с.

Відповідно, лінії звязку з роутером в 100 Мбіт/с може бути недостатньо.

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 75, то пропускна здатність мережі на рівні розподілу буде дорівнює:

Рр.р= μ*l*N*8= 161*650*75*8= 62,8 (Мбіт/с),

Де N - кількість користувачів в найбільшій мережі.

Додаємо до отриманого результату трфік 10 IP відеокамер і отримуємо:

Рр.р = 142.8 (Мбіт/с)

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде. Якщо комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000 Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

μвих=1000 000 000/(650*8)=192 307 пакетів/с

Оскільки кожне джерело виробляє в середньому 161 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

N=192307/161=1194 джерела.

З яких 75 відносяться до ПК а більше 1100 можна використати для іншого бладнання та IP відео.

Інтенсивність вихідного трафіку від всіх користувачів, якщо використовувати 20 IP відеокамер. Кожна IP відеокамера завантажує канал як 10 ПК:

λ=N*μ= (75+200)*161=44275 (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 =44275/192307=0,23

Коефіцієнт зайнятості комутатора рівня розподілу:

r=ρ/(1-ρ)=0,23/(1-0,23)=0,3

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

T=1/((μ-λ))=1/(192307-44275)=6,75 мкс

Середня довжина черги:

L_чер=ρ^2/(1-ρ)= ⟦0,23^2/(1-0,23)]=0.0687

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 [20].

Середній час перебування пакета в черзі

T_оч=L_чер/λ=0,0687/44275=1,55 мкс

Це значення менше необхідного значення ≤6 мс, що задовольняє вимогам.

Пропускна здатність каналу:

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

b=λ*l=44275*650*8= 230 Мбіт/с

Що задовольняє пропускній здатності вихідного каналу.

# 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

## 3.1 Розрахунок схеми адресації корпоративної мережі

Принцип IP-адресації - виділення множини (діапазону, блоку, підмережі) IP-адрес, в якому деякі бітові розряди мають фіксовані значення, а інші розряди пробігають всі можливі значення. Блок адрес задається вказівкою початкової адреси та маски підмережі. Безкласова адресація ґрунтується на змінній довжині маски підмережі (англ. variable length subnet mask, VLSM), тоді як у класовій (традиційній) адресації довжина маски суворо фіксована 0, 1, 2 або 3 встановленими октетами.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **LAN1** | 75 | 126 | 192.168.16.0 | /25 | 255.255.255.128 | 192.168.16.1 - 192.168.16.126 | 192.168.16.127 |
| **LAN2** | 42 | 62 | 192.168.16.128 | /26 | 255.255.255.192 | 192.168.16.129 - 192.168.16.190 | 192.168.16.191 |
| **LAN3** | 16 | 30 | 192.168.16.192 | /27 | 255.255.255.224 | 192.168.16.193 - 192.168.16.222 | 192.168.16.223 |
| **LAN4** | 12 | 14 | 192.168.16.224 | /28 | 255.255.255.240 | 192.168.16.225 - 192.168.16.238 | 192.168.16.239 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **WAN1** | 2 | 2 | 10.0.6.0 | /30 | 255.255.255.252 | 10.0.6.1 - 10.0.6.2 | 10.0.6.3 |
| **WAN2** | 2 | 2 | 10.0.6.4 | /30 | 255.255.255.252 | 10.0.6.5 - 10.0.6.6 | 10.0.6.7 |
| **WAN3** | 2 | 2 | 10.0.6.8 | /30 | 255.255.255.252 | 10.0.6.9 - 10.0.6.10 | 10.0.6.11 |
| **WAN4** | 2 | 2 | 10.0.6.12 | /30 | 255.255.255.252 | 10.0.6.13 - 10.0.6.14 | 10.0.6.15 |
| **WAN5** | 2 | 2 | 10.0.6.16 | /30 | 255.255.255.252 | 10.0.6.17 - 10.0.6.18 | 10.0.6.19 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **VLAN16** | 10 | 14 | 192.168.16.0 | /28 | 255.255.255.240 | 192.168.16.1 - 192.168.16.14 | 192.168.16.15 |
| **VLAN26** | 10 | 14 | 192.168.16.16 | /28 | 255.255.255.240 | 192.168.16.17 - 192.168.16.30 | 192.168.16.31 |
| **VLAN36** | 10 | 14 | 192.168.16.32 | /28 | 255.255.255.240 | 192.168.16.33 - 192.168.16.46 | 192.168.16.47 |
| **VLAN99** | 10 | 14 | 192.168.16.48 | /28 | 255.255.255.240 | 192.168.16.49 - 192.168.16.62 | 192.168.16.63 |

Рисунок 3.1 – Результат роботи онлайн калькулятора підмереж

Для побудови мережі ТОВ «Оптиматех» використаний адресний простір 10.23.28.0/22. Розрахунок схеми адресації виконаний згідно до завдання.

Таблиця 3.1 – Кількість вузлів в підмережах

| LAN1 | LAN2 | LAN3 | LAN4 | LAN5 |
|---|---|---|---|---|
| 62 | 12 | 85 | 42 | 34 |

В таблиці 3.2 наведена схема IP-адресації в корпоративній мережі.

Таблиця 3.2 – Схема адресації мережі

| Назва підмережі | Розмір | Адреса | Десяткова маска | Діапазон доступних адрес |
|---|---|---|---|---|
| LAN1 | 75 | 192.168.16.0 | 255.255.255.128 | 192.168.16.1 - 192.168.16.126 |
| LAN2 | 42 | 192.168.16.128 | 255.255.255.192 | 192.168.16.129 - 192.168.16.190 |
| LAN3 | 16 | 192.168.16.192 | 255.255.255.224 | 192.168.16.193 - 192.168.16.222 |
| LAN4 | 12 | 192.168.16.224 | 255.255.255.240 | 192.168.16.225 - 192.168.16.238 |
| VLAN16 | 10 | 192.168.16.0 | 255.255.255.240 | 192.168.16.1 - 192.168.16.14 |
| VLAN26 | 10 | 192.168.16.16 | 255.255.255.240 | 192.168.16.17 - 192.168.16.30 |
| VLAN36 | 10 | 192.168.16.32 | 255.255.255.240 | 192.168.16.33 - 192.168.16.46 |
| VLAN99 | 10 | 192.168.16.48 | 255.255.255.240 | 192.168.16.49 - 192.168.16.62 |
| WAN1 | 2 | 10.0.6.0 | 255.255.255.252 | 10.0.6.1 - 10.0.6.2 |
| WAN2 | 2 | 10.0.6.4 | 255.255.255.252 | 10.0.6.5 - 10.0.6.6 |
| WAN3 | 2 | 10.0.6.8 | 255.255.255.252 | 10.0.6.9 - 10.0.6.10 |
| WAN4 | 2 | 10.0.6.12 | 255.255.255.252 | 10.0.6.13 - 10.0.6.14 |
| WAN5 | 2 | 10.0.6.16 | 255.255.255.252 | 10.0.6.17 - 10.0.6.18 |

Виконана адресація усіх пристроїв в мережі ( таблиця 3.3).

Таблиця 3.3 – Схема адресації пристроїв мережі

| Им’я пристрою | Інтерфей | IP адреса | Маска | Шлюз | VLAN | Для ПК інтерфейс підключеного пристрою |
|---|---|---|---|---|---|---|
| (LAN 1) | | | | | | |
| Obolonska _ Rout2 | G0/0 | 192.168.16.1 | /25 | | | Sw1-Fa0 |
| | G0/0/16 | 192.168.16.3 | /28 | 192.168.16.1 | 16 | - |
| | G0/0/26 | 192.168.16.17 | /28 | 192.168.16.1 | 26 | - |
| | G0/0/36 | 192.168.16.33 | /28 | 192.168.16.1 | 36 | - |
| | G0/0/99 | 192.168.16.49 | /28 | 192.168.16.1 | 99 | - |
| | G0/1 | 10.0.6.1 | /30 | | | R4_G0/1 |
| | G0/2 | 10.0.6.5 | /30 | | | R1_G0/1 |
| Obolonska _ Sw1 | Vlan99 | 192.168.16.2 | /28 | 192.168.16.1 | | - |
| Server TFTP | Fa0 | 192.168.16.16 | /25 | 192.168.16.1 | | - |
| WebCam1_1-WebCam1_2 | NIC | 192.168.16.44 - 192.168.16.45 | /25 | 192.168.16.1 | | - |
| RfeedReader 1_3 | NIC | 192.168.16.46 | /25 | 192.168.16.1 | | - |
| PC16_1 – PC16_10 | NIC | 192.168.16.4 - 192.168.16.14 | /28 | 192.168.16.3 | 16 | - |
| PC26_1 – PC26_10 | NIC | 192.168.16.18 - 192.168.16.28 | /28 | 192.168.16.17 | 26 | - |
| PC36_1 – PC36_9 | NIC | 192.168.16.34 - 192.168.16.43 | /28 | 192.168.16.33 | 36 | - |
| (LAN 2) | | | | | | |
| Obolonska _ Rout4 | G0\0 | 192.168.16.129 | /26 | | | Sw5_Fa0 |
| | G0\1 | 10.0.6.2 | /30 | | | R2_G0/1 |
| | G0\2 | 10.0.6.13 | /30 | | | R3_G0/1 |
| Obolonska _ Sw5 | Vlan1 | 192.168.16.130 | /26 | 192.168.16.129 | | - |
| Пункт конторолю №1 | | | | | | |
| PC2_1-PC2_2 | NIC | 192.168.16.131- 192.168.16.132 | /26 | 192.168.16.129 | | - |
| WebCam2_1-WebCam2_15 | NIC | 192.168.16.133 - 192.168.16.148 | /26 | 192.168.16.129 | | - |
| WiredEndDevice Optex Fiber Sensys FD-342 1-4 | NIC | 192.168.16.149- 192.168.16.152 | /26 | 192.168.16.129 | | - |
| Пункт конторолю №2 | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| PC2_3-PC2_4 | NIC | 192.168.16.153 - 192.168.16.155 | /26 | 192.168.16.129 | | - |
| WebCam2_16-WebCam2_26 | NIC | 192.168.16.156 - 192.168.16.167 | /26 | 192.168.16.129 | | - |
| WiredEndDevice Optex Fiber Sensys FD-342 5-8 | NIC | 192.168.16.168 - 192.168.16.171 | /26 | 192.168.16.129 | | - |
| Server VIDEO | Fa0 | 192.168.16.145 | /26 | 192.168.16.129 | | - |
| Server DNS | Fa0 | 192.168.16.144 | /26 | 192.168.16.129 | | - |
| (LAN 3) | | | | | | |
| ISP | G0\0 | 192.168.16.193 | /27 | | | Sw4_Fa0 |
| | G0\1 | 10.0.6.17 | /30 | | | R3_G0/2 |
| | G0\2 | 209.165.200.9 | /30 | | | PC00_Fa0 |
| Obolonska _ Sw4 | Vlan1 | 192.168.16.194 | /27 | 192.168.16.193 | | - |
| PC3_1-PC3_15 | NIC | 192.168.16.195-192.168.16.210 | /27 | 192.168.16.193 | | - |
| Server HTTP | Fa0 | 192.168.16.208 | /27 | 192.168.16.193 | | - |
| (LAN 4) | | | | | | |
| Obolonska _ Rout1 | G0\0 | 192.168.16.225 | /28 | | | Sw0_Fa0 |
| | G0\1 | 10.0.6.6 | /30 | | | R2_G0/2 |
| | G0\2 | 10.0.6.9 | /30 | | | R3_G0/0 |
| Obolonska _ Sw0 | Vlan1 | 192.168.16.226 | /28 | 192.168.16.225 | | - |
| PC4_1-PC4_6 | NIC | 192.168.16.227-192.168.16.232 | /28 | 192.168.16.225 | | - |
| WebCam4_1-WebCam4_3 | NIC | 192.168.16.233-192.168.16.235 | /28 | 192.168.16.225 | | - |
| RfeedReader 1-3 | NIC | 192.168.16.236 - 192.168.16.238 | /28 | 192.168.16.225 | | - |
| | | | | | | |
| Obolonska _ Rout3 | G0\0 | 10.0.6.10 | /30 | | | R1_G0/2 |
| | G0\1 | 10.0.6.14 | /30 | | | R4_G0/2 |
| | G0\2 | 10.0.6.18 | /30 | | | ISP_G0/1 |
| PC00 | Fa0 | 209.165.200.10 | /30 | 209.165.200.7 | | ISP_G0/2 |

## 3.2 Розробка логічної схеми корпоративної мережі

Відповідно до технічних вимог до розроблюваної компютерної системи на логічній схемі компютерної мережі виділено локальну мережу LAN1 в якій розташовані підрозділи «Управління, менеджмент, серверна, допоміжні підрозділи, які обслуговують систему доступу з розпізнаванням обличчя та пропуски Rfeed технології».

Локальна мережа LAN3 обєднує мережеві пристрої дирекції підприємства.

Локальна мережа LAN4 забезпечує доступ до пунктів прпуску на територію підприємства та в цехи підприємства. Контроль забезпечується розпізнаванням обличчя та зчитуванням інформації з електронного пропуску.

Система охорони периметра обслуговується локальною мережею LAN2. Для розмежування обладнання локальної мережі використано два комутатора, до яких підєднані елементи системи контролю вібрації периметра та системи відеокамер. Відеосервер та DNS сервер розташовані в пункті контролю №2.

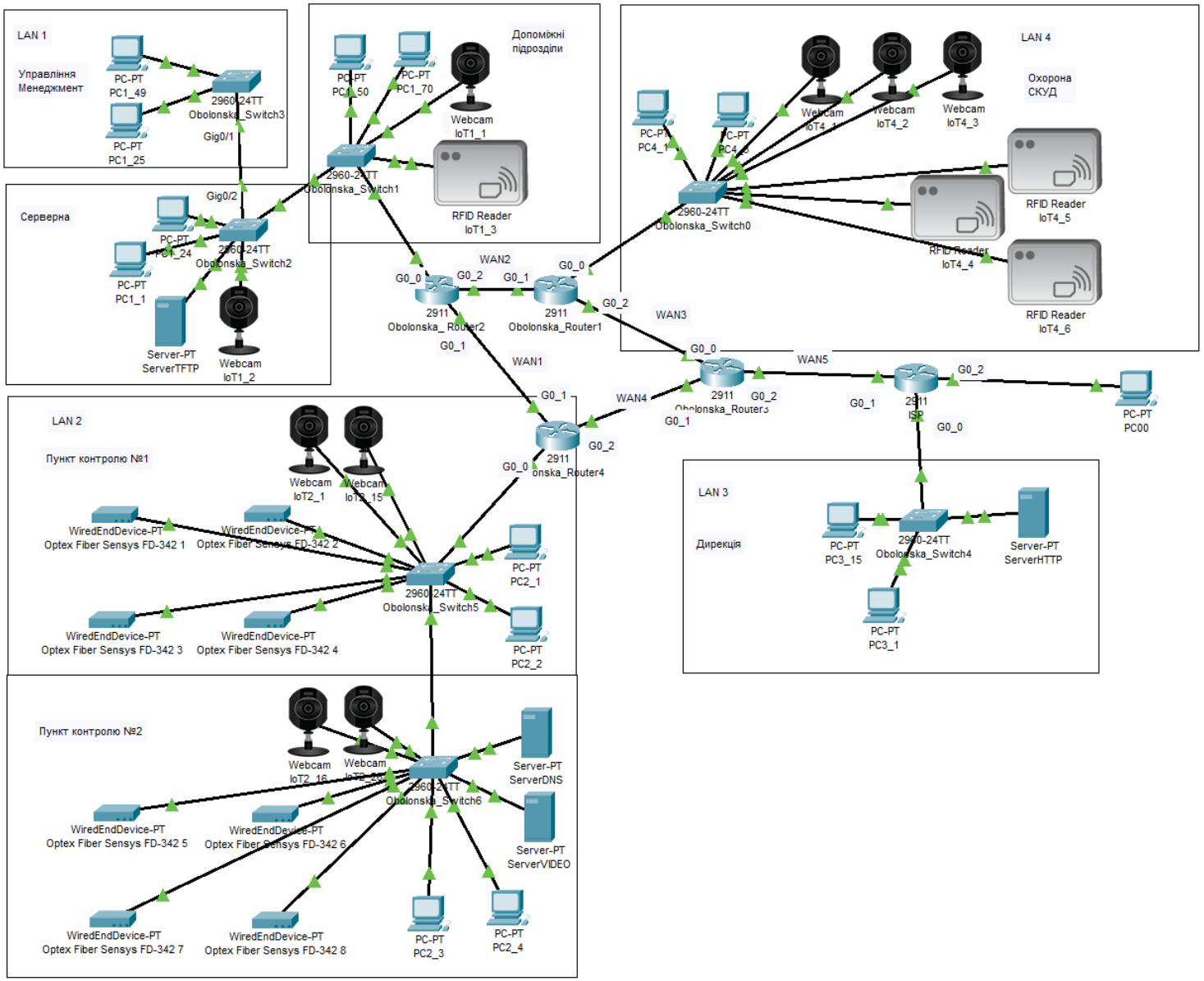


Рисунок 3.2 – Логічна схема корпоративної мережі

## 3.3 Особливості використовуваних моделей пристроїв кіберфізичної системи

Для імітації роботи контролерів Optex Fiber Sensys FD-342 5-8 у моделі мережі використано модулі WiredEndDevice. Користувальницький пристрій з дротовим підключенням. Має графічний інтерфейс користувача з редагованим HTML-кодом. Вкладка Графічний інтерфейс (GUI) має в своєму розпорядженні генератор трафіку (Traffic Generator) таким же як і у ПК і ноутбука.

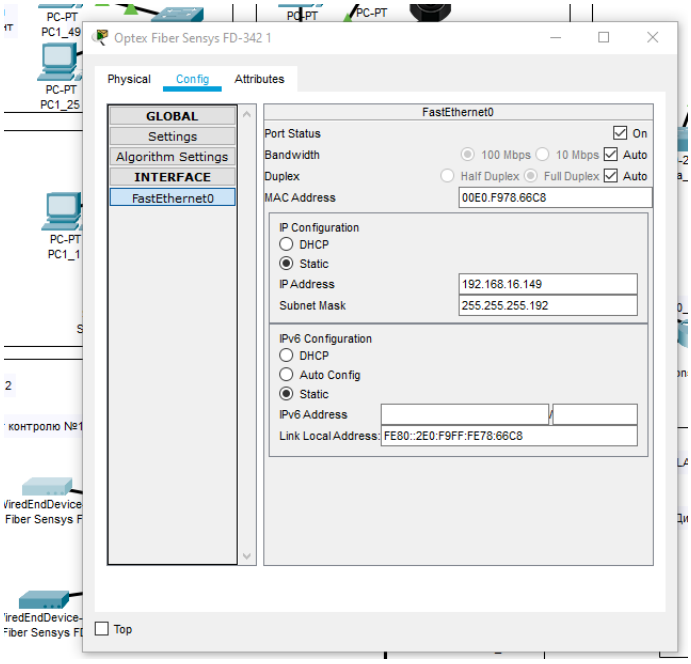


Рисунок 3.3 Пристрій та користувацький інтерфейс модуля WiredEndDevice

Також у проекті компютерної мережі використано такі пристрої як WebCam що відносяться до розділу IoT і пристрої для зчитування RfeedReader. Ці пристрої передбачені в системі контролю доступу.

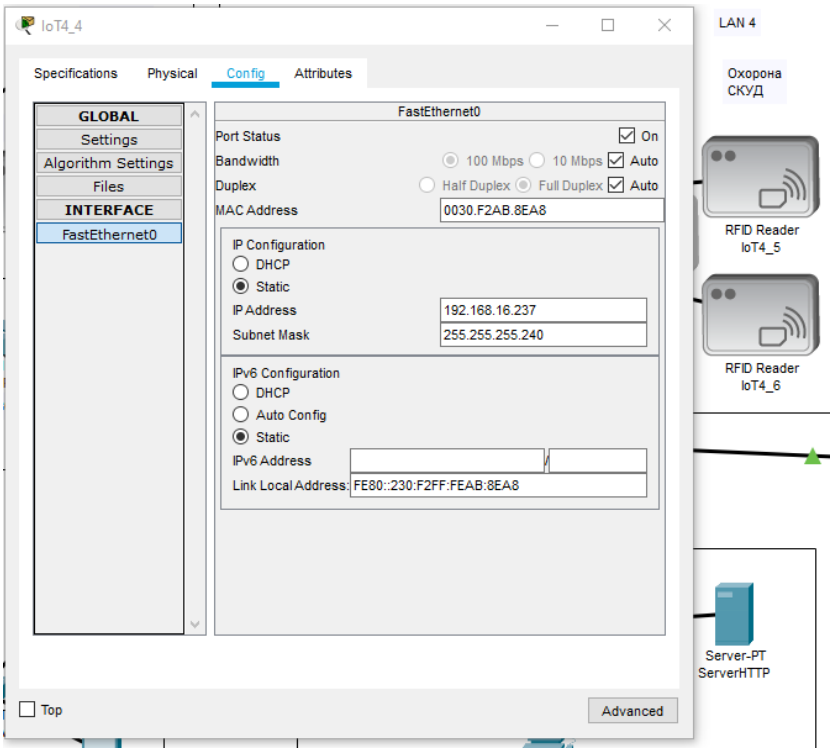


Рисунок 3.4 Пристрій та користувацький інтерфейс модуля RfeedReader

Вище описані пристрої не мають таких повних налаштувань як ПК але їх можна використовувати як імітація деякої системи, що використовується і підключена до компютерної мережі.

Окремо потрібно спинитися на особливостях реалізації кіберфізичної системи охорони периметра з урахуванням її інтеграції в компютерну систему всього підприємства.

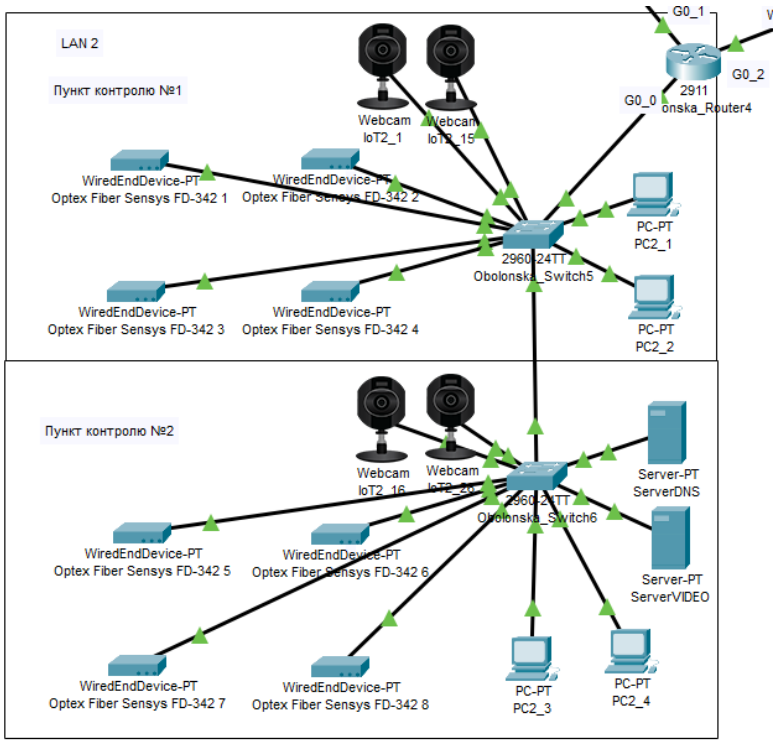


Рисунок 3.5 - Локальна мережа, що забезпечує функціонування системи охорони периметра.

Для забезпечення функціонування системи охорони периметра сервер DNS розташовується в локальній мережі LAN2.

Система DNS складається з серверів та клієнтів. DNS-сервери підтримують розподілену базу дозволів імен, а DNS-клієнти, якими є практично всі мережеві пристрої, звертаються до серверів із запитами про дозвіл доменного імені на IP-адресу. Програма, що реалізує функції клієнта DNS, називається резольвером та входить до складу операційної системи. Будь-який додаток, у якого виникає необхідність відображення доменного імені, звертається до резольвера своєї операційної системи, який взаємодіє з DNS-сервером.

DNS-сервери утворюють ієрархію, на вершині якої розташовуються кореневі сервери. Ці сервери зберігають текстові файли імен та IP-адрес DNS-серверів наступного (верхнього) рівня, які, у свою чергу, зберігають дані про імена та адреси імен, що входять до доменів верхнього рівня, а також про імена

DNS-серверів, які обслуговують домени другого рівня ієрархії і т. д. Простір доменних імен розділений між серверами, так, щоб кожен сервер зберігав записи тільки в межах одного рівня, а для імен своїх піддоменів зберігав лише посилання на сервери DNS, які відповідають за ці піддомени.

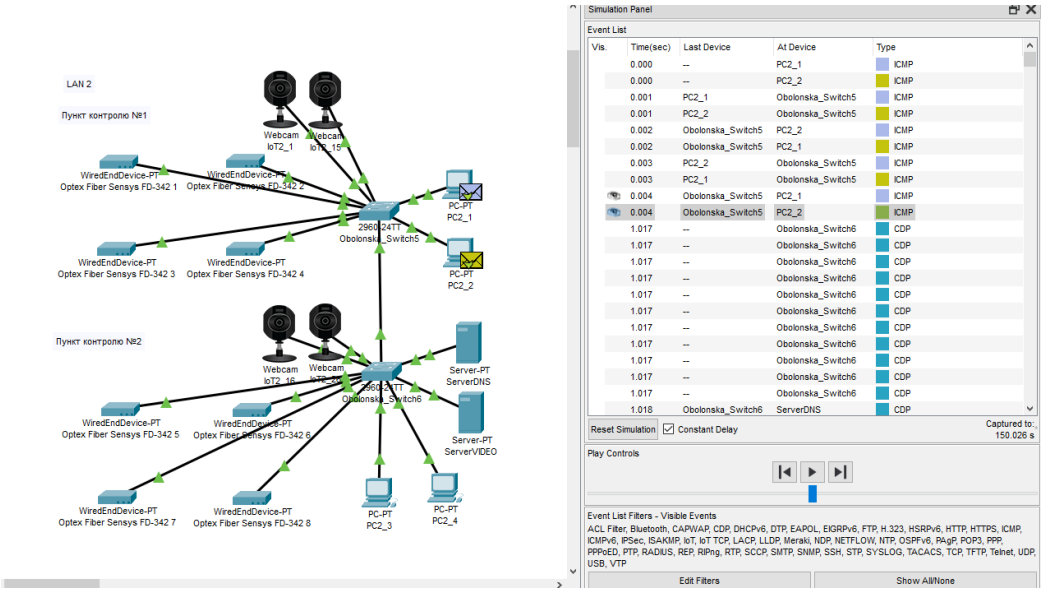


Рисунок 3.6 Робота мережі LAN2.

Тому локальна мережа, що забезпечує роботу системи охорони периметру може функціонувати навіть якщо корпоративна мережа вийде з ладу і не зможе виконувати свої функції. Периметр підприємства залишиться під охороною.

## 3.4 Налаштування та перевірка роботи комп'ютерної системи

### 3.4.1 Базове налаштування конфігурації пристроїв

Вкладка Налаштування вікна властивостей пристрою містить графічний інтерфейс для налаштування деякої кількості загальних опцій. Більше того, коли ви працюєте нашвидкуруч з графічним інтерфейсом, у нижньому вікні вкладки відображаються еквівалентні команди Cisco IOS.

На вкладці Настройка (Config) комутатора зробимо таку послідовність дій: Інтерфейс (Interface) → FastEthernet0/1 і далі приберіть в опції Статус порту

(Port Status) пташку Увімк (On). У вікні еквівалентних команд Cisco IOS (Equivalent IOS Commands) відобразяться такі команди:

- налаштування глобального режиму конфігурування;

– маршрутизацію (на маршрутизаторі чи комутаторі третього рівня);

– базу даних VLAN (на комутаторі);

- опції інтерфейсу.

```
Router(config) #hostname Obolonska_Rout1
Obolonska_Rout1(config) #no ip domain-lookup
Obolonska_Rout1(config) #service password-encryption
Obolonska_Rout1(config) #enable secret cisco
Obolonska_Rout1(config) #line conscle 0
Obolonska_Rout1(config-line) #password cisco
Obolonska_Rout1(config-line) #login
Obolonska_Rout1(config-line) #exit
Obolonska_Rout1(config) #line vty 0 15
Obolonska_Rout1(config-line) #password cisco
Obolonska_Rout1(config-line) #login local
Obolonska_Rout1(config-line)#trans inp ssh
Obolonska_Rout1(config-line) #exit
Obolonska_Rout1(config) #banner motd #123-20z Obolonska. PROTECTION
system. AAA services Authorized!#
Obolonska_Rout1(config) #username 12320z_ Obolonska password cisco
Obolonska_Rout1(config) #ip domain-name Obolonska_Rout1
Obolonska_Rout1(config) #cryp key g r
```

Рисунок 3.7 – Базове налаштування роутера Obolonska_Rout1

### 3.4.2 Налаштування протоколу EIGRP та технології NAT

Удосконалений внутрішній протокол маршрутизації шлюзів (EIGRP) – це протокол маршрутизації, що поєднує властивості дистанційно-векторних протоколів і протоколів за станом каналу зв'язку.

Для роботи EIGRP використовує 5 типів повідомлень:

hello – маршрутизатори використовують широкомовні hello-пакети без підтвердження виявлення сусідів;

update – повідомлення, які містять інформацію про зміну маршрутів, надсилаються тільки маршрутизаторам, яких стосується оновлення;

query – коли маршрутизатор виконує підрахунок маршруту і він не має feasible successor, він відправляє query-пакет своїм сусідам у тому щоб визначити чи немає feasible successor цього пункту призначення вони;

reply – маршрутизатор відправляє reply-пакет у відповідь query-пакет;

ACK – пакет, який підтверджує отримання пакетів update, query та reply.

```
Obolonska_Rout1(config)#router eigrp  2
*Mar 1 0:2:0.287: %SSH-S-ENABLED: SSH 1.99 has been enabled
Obolonska_Rout1(config-router) #redistribute static
Obolonska_Rout1(config-router) #no auto-sumary
Obolonska_Rout1(config-router) #network 192.168.16.224 0.0.0.3
Obolonska_Rout1[config-router) #network 10.0.6.4 0.0.0.3
Obolonska_Rout1(config-router) #network 10.0.6.8 0.0.0.3
Obolonska_Rout1(config-router) #pas g0/0
Obolonska_Rout1(config-rowter) #exit
Obolonska_Rout1(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.4
```

Рисунок 3.8 – Налаштування протоколу EIGRP 4 на Obolonska_Rout1

Мережева технологія NAT активно застосовується в корпоративних та гостьових мережах і призначена для:

економії кількості статичних IP-адрес,

забезпечення безпеки пристроїв усередині локальної мережі,

запобігання зверненням ззовні до внутрішніх хостів,

дозволяє приховати внутрішню структуру корпоративної мережі зовнішнього спостерігача.

Функція NAT DNS служить для прив'язки різних профілів фільтрації сервісу SkyDNS до різних пристроїв за NAT (роутерів, точок доступу, інтернет-шлюзів тощо).

Статичний NAT відображає локальні IP-адреси на конкретні публічні адреси на основі один одного. Застосовується, коли локальний хост має бути доступний ззовні з використанням фіксованих адрес.

Кроки налаштування технології NAT на роутері Dvoradkin_R3.

```
Obolonska_Rout3(config) access-list 4 permit 10.0.6.8 0.0.3.255
Obolonska_Rout3(config) #ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
 Obolonska_Rout3(config) #ip nat inside source list 4 pool Internet
 Obolonska_Rout3(config)#ip nat inside source static 10.0.6.12 209.165.200.6
 Obolonska_Rout3(config)#ip route 0.0.0.0 0.0.0.0 205.165.200.5
 Obolonska_Rout3(config)#ip route 10.0.6.16 255.255.252.0 so/o/o
 Obolonska_Rout3(config) #interface g0/2
 Obolonska_Rout3(config-if)#ip nat outside
 Obolonska_Rout3(config-if) #interface g0/1
 Obolonska_Rout3(config-if)#ip nat inside
 Obolonska_Rout3(config-if) #interface g 0/0
 Obolonska_Rout3(config-if)#ip nat inside
```

Рисунок 3.9 – Налаштування NAT роутері Dvoradkin_R3

### 3.4.3 Перевірка роботи комп’ютерної системи

Симулятор Packet Tracer є інтегрованим середовищем моделювання комп'ютерної мережі. Він допомагає створювати мережеві моделі, здійснювати візуалізацію та анімацію передачі в мережі.

Однак, як і будь-яке середовище моделювання, Packet Tracer спирається на спрощені моделі мережевих пристроїв та протоколів, мережеві протоколи, реалізовані у Packet Tracer.

У режимі симуляції (Simulation) можна вивчати роботу мережі у повільному темпі, досліджуючи шляхи, якими пересилаються пакети.

При перемиканні в режим моделювання з'явиться спеціальна панель. Можна графічно переглядати розповсюдження пакетів через мережу, якщо натиснути на кнопку Add Simple PDU.

Є можливість контролю швидкості моделювання за допомогою кнопки Speed Slider. Також можна переглядати попередні події, натиснувши кнопку Back.

Вузол, який отримав пакет, для нього не призначений, цей пакет повинен проігнорувати, виняток можливий у тому випадку, якщо на вузлі встановлено спеціальне програмне забезпечення – сніффер.

Вузол-одержувач при надходженні пакета ICMP надсилає відповідь.

Вузол-відправник отримує його, вимірює затримку між відправленням та отриманням пінгу та формує звіт.

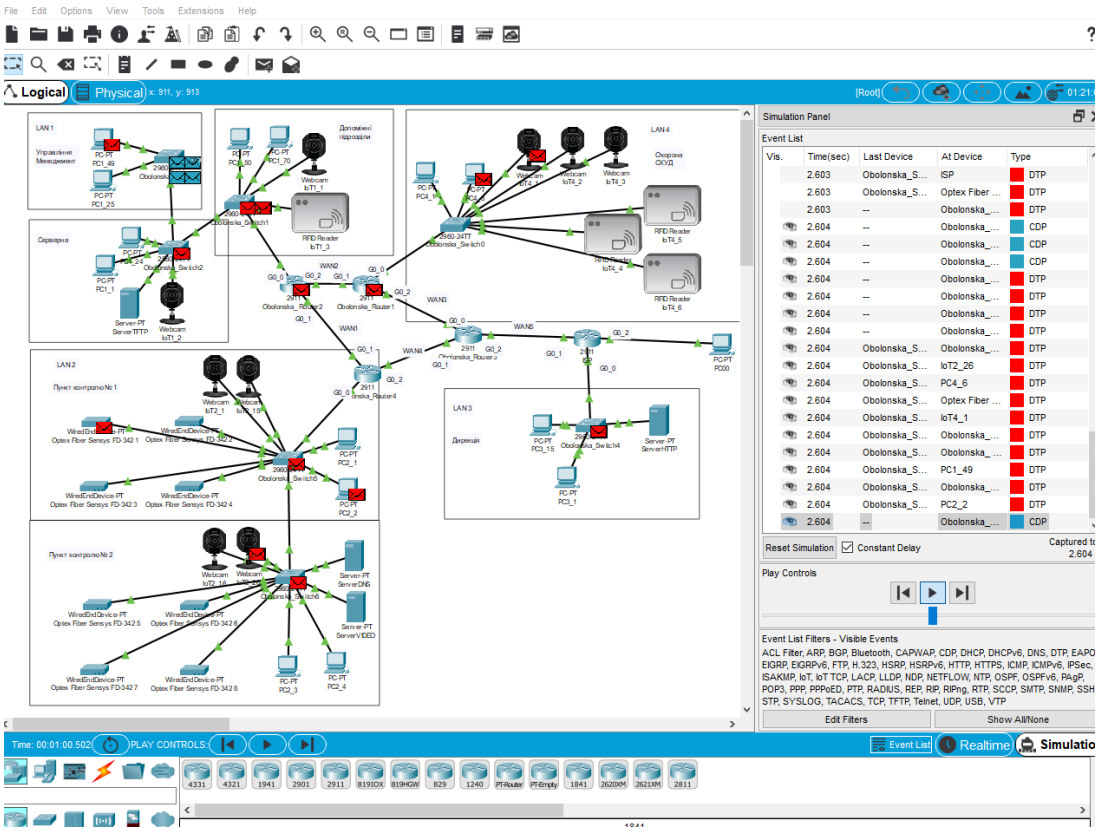


Рисунок 3.10 – Режим симуляції

## 3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

### 3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Програмні методи захисту – це сукупність алгоритмів та програм, що забезпечують розмежування доступу та виключення несанкціонованого використання інформації.

Сутність методів захисних перетворень полягає в тому, що інформація, що зберігається в системі і передається каналами зв'язку на фізичному рівні моделі OSI, представляється в деякому коді, що виключає можливість її безпосереднього використання.

Прикладний рівень надає послуги користувачам програм – доступ до загальних мережевих ресурсів (файлів, принтерів або вебсторінок) або розподілених мережевих сервісів (електронної пошти, служб передачі повідомлень, баз даних). Як правило, послуги прикладного рівня включають ідентифікацію та аутентифікацію учасників мережевої взаємодії, перевірку їх доступності та повноважень, визначення вимог до захищеності сеансу обміну. Для запитів на прикладний рівень використовуються системні виклики операційної системи, що утворюють API.

### 3.5.2 Налаштування служби AAA

У мережевих технологіях прийнято застосовувати строгу аутентифікацію, в процесі якої використовуються методи шифрування, а аутентифікатор не передається через мережу у відкритому вигляді. Замість автентифікатора може використовуватися його хеш-код, отриманий внаслідок односторонньої функції хешування.

Для реалізації віддаленої автентифікації у мережах використовуються протоколи автентифікації.

```
Obolonska_Rout3(config)#aaa new-model
Obolonska_Rout3(config)#aaa authentication login default local
Obolonska_Rout3(config)#aaa authentication login Login group radius local
Obolonska_Rout3(config)#line vty 0 4
Obolonska_Rout3(config-line)#login authentication default
Obolonska_Rout3(config-line)#radius-server host 192.168.16.5 auth-port 1645
Obolonska_Rout3(config)#radius-server key zzz
Obolonska_Rout3(config)#aaa authentication login SSH-LOGIN local
Obolonska_Rout3(config)#line vty 0 4
Obolonska_Rout3(config-line)#login authentication SSH-LOGIN
Obolonska_Rout3(config-line)#transport input ssh
Obolonska_Rout3(config-line)#exit
Obolonska_Rout3(config)#
Obolonska_Rout3(config)#@conft t
Obolonska_Rout3(config)#radius-server host 192.168.16.5
Obolonska_Rout3(config)#radius-server key zzz
Obolonska_Rout3(config)#aaa authentication login default group radius local
```

Рисунок 3.11 – Конфігурація служби AAA на маршрутизаторі Obolonska_Rout3

### 3.5.3 Налаштування мереж VLAN

Комутатори розбивають колізійний домен на безліч дрібних, а також є єдиним широкомовним доменом.

Віртуальні локальні мережі VLAN (Virtual LAN) уможливлюють так, що на одному комутаторі ми отримуємо безліч широкомовних доменів. Однак створивши на одному комутаторі безліч VLAN, ми зіткнемося зі стомлюючою роботою для поширення цієї конфігурації на всі інші комутатори. Таким чином, ми отримуємо безліч комутаторів з розрізненими налаштуваннями VLAN. Тут стане в нагоді протокол VTP (VLAN Trunking Protocol). Тепер маючи VLAN та протокол VTP, ми робимо керування простим. Для цього ми розглянемо маршрутизацію між віртуальними мережами (InterVLAN).

Віртуальні локальні мережі VLAN – технологія, що передбачає розбиття простої мережі другого рівня на множину широкомовних доменів. Це обмежує мережеву взаємодію лише пристроями, які знаходяться в тому самому широкомовному домені. При цьому пристрої можуть взаємодіяти, але за допомогою пристрою третього рівня, таких як маршрутизатори або комутатори

третього рівня. У загальному випадку це нагадує підключення пристроїв до різних комутаторів, а потім з'єднання комутаторів через маршрутизатор як окремих широкомовних доменів (підмереж).

Чим більше і більше створюється VLAN, тим стомливішим стає реплікація (поширення) конфігурації на всі комутатори мережі. Саме тому було створено магістральний протокол VLAN (VLAN Trunking Protocol, VTP).

```
Obolonska_Sw1(config)#vlan 16
Obolonska_Sw1(config-vlan)#name Top_menedgment
Obolonska_Sw1(config-vlan)#vlan 26
Obolonska_Sw1(config-vlan)#name Finance
Obolonska_Sw1(config-vlan)#vlan 36
Obolonska_Sw1(config-vlan)#name Buhgalteria
Obolonska_Sw1(config-vlan)#vlan 99
Obolonska_Sw1(config-vlan)#name Service
Obolonska_Sw1(config-vlan)#vlan 1
Obolonska_Sw1(config-vlan)#name Native
Obolonska_Sw1(config-vlan)#exit
```

Рисунок 3.12 – Створення VLAN

```
Obolonska_Sw1(config)#int r f0/11-18
Obolonska_Sw1(config-if-range)#sw m a
Obolonska_Sw1(config-if-range)#no shut
Obolonska_Sw1(config-if-range)#sw a v 18
Obolonska_Sw1(config-if-range)#
```

Рисунок 3.13 – Переведення портів в режим доступу

```
Obolonska_Sw1(config)#int g0/0
Obolonska_Sw1(config-if)#switchport mode trunk
Obolonska_Sw1(config-if)#switchport trunk native vlan 1
Obolonska_Sw1(config-if)#switchport trunk allowed vlan
16,26,36,99
Obolonska_Sw1(config-if)#no shutdown
```

Рисунок 3.14 – Налаштування транку

# 4 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

## 4.1 Можливості сучасних СКУД

Система контролю доступу з використанням біометричних даних особи може використовуватися як окремо, так і спільно з іншими ідентифікаторами СКУД.

Доступ на територію з розпізнавання особи є системою контролю доступу, де як ідентифікатор використовується біометричне зображення особи (або як додаткова ідентифікація). Структурна схема СКУД є стандартною, але іншими є зчитувачі: термінал розпізнавання особи.

Якщо купити та встановити СКУД за розпізнаванням особи можна або повністю відмовитися від використання пластикових карток, або, навпаки, підвищити безпеку на об'єкті завдяки подвійній ідентифікації: по карті та особі. Система розпізнавання облич настроюється централізовано на сервері. Тут можна встановити точність збігу, дистанцію спрацьовування, режим ідентифікації та інші параметри. Термінал розпізнавання облич R20-Face має захист від підробок: пройти по роздрукованій фотографії не вийде.

Термінал R20-Face (8W) – це пристрій для розпізнавання облич та ідентифікації користувачів у системі контролю доступу. Користувачеві достатньо лише на секунду подивитися на дисплей терміналу, і, за наявності відповідних прав, доступ буде дозволено. Висока швидкість розпізнавання обличчя (менше 1 секунди) дозволяє встановлювати термінал навіть у точках доступу з великим трафіком, наприклад на прохідних.

Дві вбудовані відеокамери з роздільною здатністю 2.0 Мп. розпізнають "підробки". Прилад безпомилково визначає, знаходиться перед ним реальна людина, або це лише його фотографія на папері або екрані телефону. Це дозволить уникнути фальсифікацій та незаконних проникнень на об'єкт.

Завдяки вбудованому підсвічуванню можна встановлювати термінал у приміщеннях з будь-яким ступенем освітленості, у тому числі й у повністю неосвітлених. Датчик руху зафіксує наближення людини та включить основне підсвічування [11,12].

У складі СКУД «Guard» використовується термінал підключений до мережі Ethernet, а також до контролерів Wiegand або RS-232. ПЗ по мережі здійснює повне конфігурування терміналу, а також автоматично підтримує базу даних терміналу в актуальному стані. При розпізнаванні особи код передається до контролера, який здійснює подальшу його обробку та управління виконавчим механізмом. У разі відсутності зв'язку з сервером Термінал-Контролер продовжує працювати автономно, виходячи з раніше занесених даних. Після відновлення зв'язку з сервером всі зміни, зроблені за період відсутності зв'язку, заносяться до терміналу та контролера.

У складі СКУД стороннього виробника режим аналогічний винятком того, що імпорт даних з БД сторонньої СКУД до терміналу здійснюється через спеціальну утиліту. При цьому в СКУД далі відображаються події входу та виходу працівників через точку доступу, обладнану терміналом розпізнавання осіб.

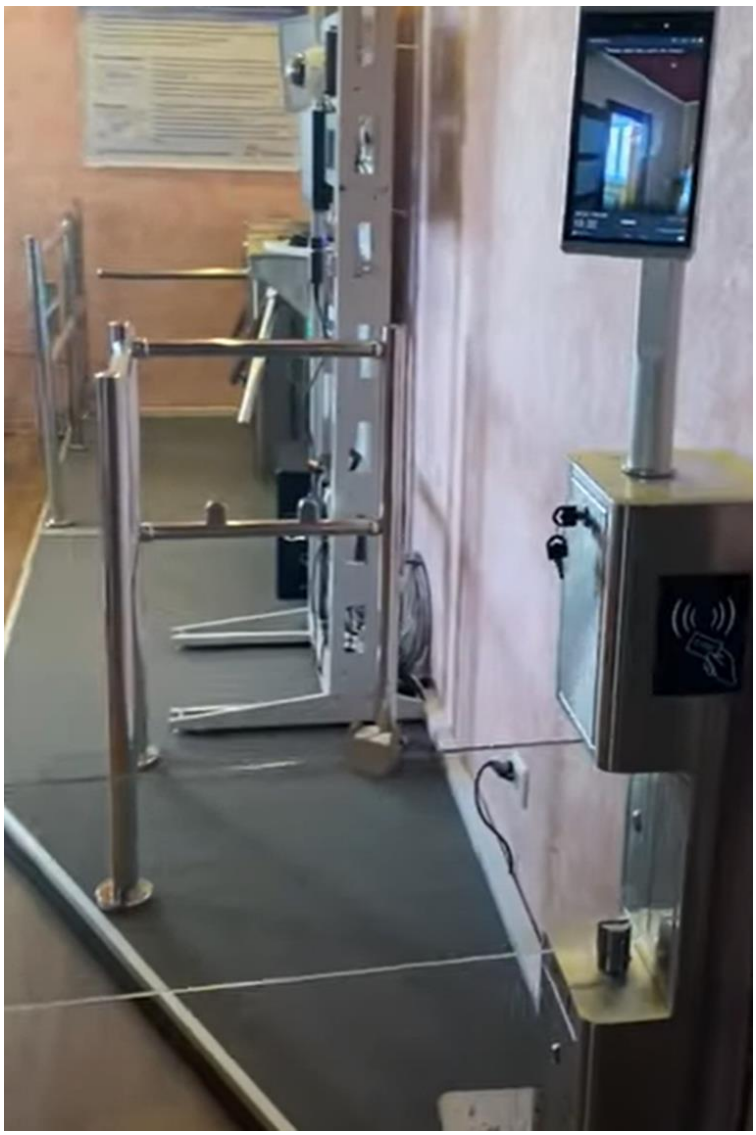

Рисунок 4.1 – СКУД з розпізнаванням обличчя

Напівавтономний режим роботи. У термінал можна вручну імпортувати дані зі звичайної таблиці Excel. Для цього потрібне з'єднання терміналу через Ethernet із ПК. Після імпорту даних термінал встановлюється на точці доступу, безпосередньо підключається до виконавчого пристрою (турнікет, двері) і керує ним за допомогою реле. Якщо потрібно додати нові дані до терміналу, процедуру імпорту потрібно повторити.

Автономний режим роботи Термінал може працювати абсолютно автономно, без зв'язки зі стороннім ПЗ або підключення до ПК. Всі дані про

співробітників вводяться на терміналі з використанням тачскрину. Інтерфейс дозволяє ввести дані співробітника і відразу зробити його еталонне фото. Термінал безпосередньо підключається до виконавчого пристрою (двері, турнікет) та керує ним за допомогою реле.

Інтеграційна платформа відеоменеджменту дозволяє керувати системами безпеки як локальних, так і територіально-розподілених об'єктів, поєднуючи тисячі камер відеоспостереження, широкий спектр охоронних систем, систем контролю та інші апаратні засоби в єдиний комплекс, забезпечуючи повнофункціональне використання мультивендорного парку обладнання.

## 4.2 Інтеграція СКУД в компютерну систему підприємства

Інтеграційні можливості.

Вибравши необхідні пристрої, побудувати в системі ISS дерево обладнання СКУД;

За вибраними пристроями передавати в систему ISS всі події, що відбуваються в СКУД;

Зчитувати в повну конфігурацію системи ISS для побудови зв'язок "Протокол подій - Робочий стіл - Камера", що використовуються для переходу за подією до архіву та перегляду асоційованого відеофрагменту.

В ISS інтегровані пристрої СКУД можна розміщувати на плани, управляти ними безпосередньо з планів, використовувати в рамках скриптів реакцій макросів для побудови складних алгоритмів взаємодії.

Використовуючи функціонал пошуку подій в ISS, можна знайти потрібне і відразу перейти до архіву для перегляду пов'язаного відеофрагменту.

Події можна фільтрувати за пристроями, типами подій (тривожною, інформаційною тощо) та підтипами подій (Вхід, Вихід і т.д.)

Використовуючи спільне рішення з ISS, можна побудувати повномасштабний ситуаційний центр моніторингу та управління, який дозволить

оперативно оцінювати обстановку на об'єктах, отримувати інформацію про події та інциденти в реальному часі.

Модуль розпізнавання автономерів.

Можливості системи:

Інтеграція зі СКУД за допомогою скриптів та макрокоманд.

Управління будь-якими точками доступу із системи ISS.

Розпізнавання номерних знаків автомобілів, що рухаються.

Автоматична реєстрація транспорту, що в'їжджає/виїжджає, із занесенням до бази даних встановлених параметрів (номер, марка, дата, час в'їзду транспортного засобу тощо).

Розпізнавання реєстраційних номерних знаків різних країн із можливістю адаптації до роботи з новими стандартами.

Оповіщення операторів та реакції компонентів системи безпеки за результатами розпізнавання.

Модуль розпізнавання облич

Можливості системи:

Інтеграція зі СКУД RusGuard за допомогою скриптів та макрокоманд.

Управління будь-якими точками доступу із системи ISS.

Автоматична реєстрація персоналу та відвідувачів.

Ідентифікація осіб.

Створення фототеки.

Збереження інформації у базі даних.

Оповіщення операторів та реакції компонентів системи безпеки за результатами розпізнавання.

ALPHAOPEN - ПЗ для організації моніторингу та управління системами безпеки та інженерними системами будівель, що застосовується на комерційних, державних та приватних об'єктах. Використовуючи сучасні методи розробки програмного забезпечення, рішення ALPHAOPEN інтегрують все охоронне

обладнання та контролери автоматизації будівель у єдину глобальну інтелектуальну систему ситуаційного контролю реального часу.

Alphalogic® PSIM дозволяє підключати до єдиного комплексу системи різних виробників, як російських, так і міжнародних.

Завдяки централізованому збору даних з усіх систем безпеки об'єкта, а також інтеграції з інформаційними системами Alphalogic® PSIM дає максимально повну картину ситуації, дозволяючи оперативно і правильно прийняти рішення про реакцію на інцидент.

Система правил і взаємодій дозволяє визначити сценарії реагування та алгоритми обробки подій будь-якої складності як в автоматичному режимі (для виключення фактора людської помилки), так і за участю операторів, що приймають рішення. Правила можуть враховувати дані від усіх інтегрованих систем, а також використовувати математичні та логічні функції, що дозволяє створювати ефективні комбіновані сценарії.

Якісна візуалізація дозволяє оперативно оцінити ситуацію на багатоекранних інтерфейсах (матриця моніторів, відеостіна) будь-якої конфігурації з детальним відображенням подій на картах або планах об'єкта в реальному часі [22].

Контроль та управління можливі як зі стаціонарних робочих місць диспетчера/оператора, так і з мобільних пристроїв – ноутбуків, планшетів, мобільних телефонів.

Можливості контролю та керування визначаються правами доступу, які можна встановити для кожного користувача системи.

Усі події та дані, що надходять від інтегрованих систем, а також дії операторів зберігаються у цифрових архівах, що дозволяє проводити розбір інцидентів, визначати взаємозв'язок та послідовність подій, а також отримувати звіти у необхідних форматах.

VisitorControl – ефективна система реєстрації, обліку та контролю відвідувачів на підприємстві.

Рішення на базі системи контролю та управління доступом RusGuard та системи бюро пропусків VisitorControl є програмно-апаратним комплексом для гнучкої автоматизації процесів контролю відвідувачів на будь-яких об'єктах рівня підприємств, бізнес центрів, офісних або інших будівель з урахуванням їх вимог до системи пропусків та особливостей інфраструктури ( будівлі, прохідні, ресепшн, організаційні структури підприємств та ін.).

Автоматизація проходу за допомогою СКУД та VisitorControl дозволяє:

створити комфортні умови прийому відвідувачів;

розвантажити бюро перепусток (реєстрація відвідувачів займає в середньому 12-15 секунд);

посилити безпеку офісу.

Основні завдання модуля інтеграції:

Реєстрація у VisitorControl відмітки про ВХІД відвідувачів на територію.

Для реєстрації події входу мало факту видачі йому пропуску, т.к. не

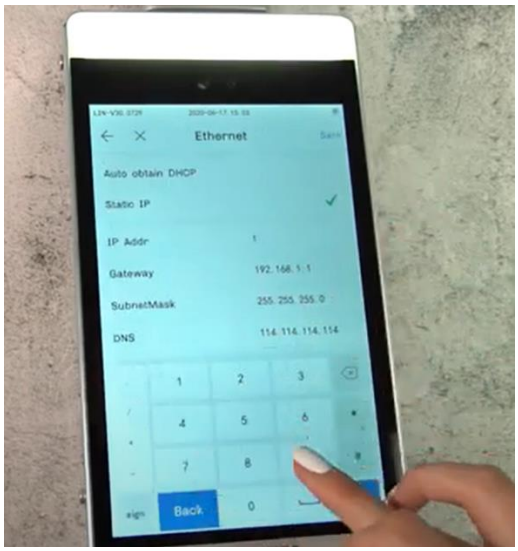


Рисунок 4.2 – Управління терміналом через Ethernet.

Ця функція забезпечує отримання даних про вхід відвідувача на об'єкт та автоматичне проставлення відповідної позначки до його електронного пропуску.

Реєстрація у VisitorControl відмітки про вихід відвідувачів з території.

Отримання зі СКУД даних про вихід відвідувача з території, що охороняється, та автоматичне проставлення відповідної позначки в його електронний пропуск.

Подією виходу з території вважається докладання картки до зчитувача або опускання картки в картоприймач.

Активація в СКУД гостьової карти тільки після реєстрації відвідувача VisitorControl.

Інтеграція передбачає, що карти для відвідувачів у СКУД заведені, але знеособлені та мають рівень доступу, що «забороняє». Після оформлення пропуску у VisitorControl інтегратор автоматично надає карті «Гостьовий» рівень доступу.

Деактивація гостьової карти до СКУД після виходу відвідувача.

Після повідомлення інтегратора про вихід відвідувача карта знеособлюється в СКУД, їй присвоюється рівень доступу, що «забороняє», що виключає можливість повторного її використання постителем без перереєстрації в VisitorControl.

Передача ПІБ відвідувача до СКУД.

Передача прізвища, імені та по батькові відвідувача до СКУД під час процесу активації картки. Це дозволяє переглядати події в СКУД за певним відвідувачем, а не лише за номером картки.

Передача фотографії відвідувача до СКУД.

Передача фото відвідувача до СКУД у процесі активації картки. Фотографія, передана в СКУД, відображається засобами системи на контрольних моніторах служби безпеки об'єкта.

1. Інтеграція рішення «БІТ:Управління доступом 8» зі СКУД RusGuard призначена для контролю доступу співробітників, аналізу відвідуваності та розрахунку відпрацьованого часу. Програма дозволяє обмежувати доступ на об'єкт, контролювати присутність працівників на робочому місці та розраховувати заробітну плату на основі отриманих даних.

2. Рішення «ФОРМУЛУ: Модуль «Облік робочого часу» зі СКУД RusGuard призначено для розширення типового функціоналу конфігурацій 1С в частині управлінського обліку подій входу-виходу співробітників організацій на територію підприємства та заповнення табелів обліку робочого часу на основі даних про реальну присутність співробітників місцях.

Модуль є зовнішню обробку до конфігурацій «Підприємство», не вимагає програмування і відразу готовий до роботи.

Застосування модуля УРВ дозволяє:

знизити трудомісткість складання табеля обліку робочого дня у конфігураціях;

прив'язати оплату праці співробітників до реальних даних про їхню присутність на робочих місцях;

знизити вплив людського чинника складання табелів обліку робочого дня.

Функціонал модуля УРВ дозволяє:

Передавати дані про організаційну структуру, кадровий склад підприємства до СКУД;

Враховувати різні варіанти розрахунку табеля для різних графіків роботи (всі входи виходи, перший вхід останній вихід);

Використовувати дані місцевих відряджень працівників;

Заповнювати стандартний документ конфігурацій "Регламентований табель обліку робочого часу" розрахованими даними.

# ВИСНОВКИ

В роботі розроблено проект удосконаленої компютерної системи підприємства ТОВ «Оптиматех».

В роботі приділена основна увага розробці корпоративної компютерної мережі з урахуванням розробки сучасної системи охорони периметра хімічного підприємства.

1. Проаналізовані особливості роботи хімічного підприємства. Показано, що підприємство велике, складне і має багато систем – система автоматичного управління технологією виробництва, система управління підприємством, особливу увагу приділено питанням безпеки.
2. Відповідно до особливостей підприємства розроблена структура системи охорони периметра. Визначена кількість вузлів, які необхідно зарезервувати для забезпечення її повноцінного функціонування.
3. Розроблена компютерна мережа підприємства та обрані сучасні технічні засоби для її реалізації..
4. Відповідно до структури компютерної мережі розроблена адресація усіх пристроїв мережі.
5. За допомогою пакету Cisco Packet Tracer розроблена модель мережі, перевірено розробку адресації та промодельовано мережу.
6. Сучасне технічне обладнання дозволяє розширити можливості мережі без змін в конфігурації і без заміни технічних засобів.
7. Додатково приведене обгрунтування використання СКУД з розпізнаванням обличчя та інтеграції до існуючої компютерної системи.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Види датчиків руху: [Електронний ресурс]. URL: https://rozetkaonline.ua/poleznie-stati-o-rozetkah-i-vikluchateliah/item/54- (дата звернення: 28.03.24)

2. . http://5fan.ua/wievjob.php?id=39490 Проектування системи аналізу технічного захисту і фізичної охорони об'єкта (на прикладі ТОВ «Ласунка»)

3. Михайлюк О.П. Теоретичні основи пожежної профілактики технологічних процесів та апаратів: навч. посібник /О.П. Михайлюк, В.В. Олійник, Г.О. Мозговий. – Харків: АЦЗУ, 2004.– 407 с.

4. Журавська І. М. Проектування та монтаж локальнихкомп'ютернихмереж :[навчальнийпосібник] / І. М. Журавська. – Миколаїв :Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.

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

6. Аналогові і цифрові системи відеонагляду(Електрон. ресурс) / Спосіб доступу: URL:http://elites-montage.com.ua/svanalog.php. - Загол. з екрана.

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

8. IP Калькулятор [Електронний ресурс] – Режим доступу : URL : http://ip-calculator.ua/. – Загол. з екрана.

9. VLSM Calculator – калькулятор під мереж з маскою змінної довжини [Електронний ресурс]. – Режим доступа:URL:http://www.vlsm-calc.net/. – Загол. з екрана.

10. ДСТУ4030-2001. Позначення умовні графічні та літерні. Системи охоронного призначення – Київ.: Держстандарт України,2001. – 115 с.

11. Підручник з інформатики – захист інформації в інформаційних системах. Спосіб доступу: URL: http://pidruchniki.ws/ 13670622 /informatika/zahist_ informatsiyi_ informatsiynih_sistemah , Загол. з екрана;

12. НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання обєктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»;

13. Надійність комп’ютерних систем Тарасенко В.П., Маламан А.Ю., Черніченко Ю.П., Корнійчук В.І.. – Навч. посібник. - К.: "Корнійчук", 2007. - 256 с. - ISBN 966-7599-37-X.

14. ДСТУ 3396.1-96 Державний стандарт України «Захист інформації. Технічний захист інформації. Порядок проведення робіт»

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

16. 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.

17. Глухов В.С., Костик А.Т. Дослідження та проектування комп’ютерних систем та мереж. – К.: Магнолія., 2023. – 253 с.

18. Б.І. Масловський, В.І. Дрововозов, О.В. Коба Технології проектування комп'ютерних систем. – К: НАУ, 2015. – 500 с.

19. Парамуд Я.С. Периферійні пристрої, інтерфейси та драйвери. – К.: Магнолія, 2023. – 210 с.

20. Білова М.О., Євсеєв С.П., Жученко О.С. Технологія Ethernet. Лабораторний практикум. – К.: Новий світ-2000, 2024. – 196 с.

21. Микитишин А.Г. та інші.Комп'ютерні мережі. Книга 2. – К.: Магнолія, 2013. – 328 с.

22. Розробка программного 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.

23. Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, підзаг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с.

24. Комп’ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп’ютерна інженерія /Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.

# ДОДАТОК А

Текст програми налаштування мережі комп’ютерної системи

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

# ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24006-01 12 01

Листів 9

Дніпро

2024

# АНОТАЦІЯ

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

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

# ЗМІСТ

**1. Скрипт налаштування ISP**

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

license udi pid CISCO2911/K9 sn FTX1524MG9C-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.16.193 255.255.255.224
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.6.17 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 209.165.200.9 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip flow-export version 9
no cdp run
!
line con 0
line aux 0
line vty 0 4
 login
end
```

**2. Скрипт налаштування Obolonska Router1**

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524NI6L-
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.16.225 255.255.255.240
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.6.6 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.6.9 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
no cdp run
!
line con 0
line aux 0
line vty 0 4
 login
!
End
```

**3. Скрипт налаштування Obolonska Router2**

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524K7WH-
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.16.1 255.255.255.128
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.6.1 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.6.5 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
!
no cdp run
!
line con 0
line aux 0
line vty 0 4
 login
!
End
```

**4. Скрипт налаштування Obolonska Router3**

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX152402FE-
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 10.0.6.10 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.6.14 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.6.18 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip flow-export version 9
no cdp run
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

**5. Скрипт налаштування Obolonska Router4**

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524824S-
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.16.129 255.255.255.192
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.6.2 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.6.13 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
!
```

```
no cdp run
line con 0
line aux 0
line vty 0 4
 login
!
end
```