

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

Інститут електроенергетики

(інститут)

Факультет інформаційних технологій

(факультет)

Кафедра інформаційних технологій та комп'ютерної інженерії

(повна назва)

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

студента Єщенко Станіслава Олександровича _____
(ПІБ)

академічної групи 123М-19-1 _____
(шифр)

спеціальності 123 «Комп'ютерна інженерія» _____
(код і назва спеціальності)

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

на тему «Обґрунтування структури та параметрів комп'ютерної системи відеоспостереження дата-центру компанії «Датасфера» з детальною розробкою сервера бази даних відеоконтенту»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Ткаченко С.М			
розділів:				
теоретичний розділ	доц. Ткаченко С.М			
синтез системи	доц. Ткаченко С.М			
розроблення програмного забезпечення	ас. Бешта Л.В			
експериментальний розділ	доц. Ткаченко С.М.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

**Дніпро
2020**

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

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

«___» грудня 2020 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр
(бакалавра, спеціаліста, магістра)

студенту Єщенко С. О. академічної групи 123М-19-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему «Обґрунтування структури та параметрів комп'ютерної системи
відеоспостереження дата-центру компанії «Датасфера» з детальною розробкою
сервера бази даних відеоконтенту,

затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 р. № 888-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел формулювання завдання, конкретизування предмету та мети роботи	01.11.2020
Синтез системи	Розробка комп'ютерної системи	01.11.2020
Програмний розділ	Розробка програмного забезпечення	01.11.2020
Експериментальний	Проведення і обробка результатів експериментів	01.12.2020

Завдання видано _____
(підпис керівника)

доц. Ткаченко С.М.
(прізвище, ініціали)

Дата видачі 01 жовтня 2020 р.

Дата подання до екзаменаційної комісії

10.12.2020 р.

Прийнято до виконання _____
(підпис студента)

Єщенко С. О.
(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: _____ с., _____ рис., _____ табл., _____ дод., _____ джерел.

Об'єкт дослідження: система відеоспостереження дата-центру компанії «Датасфера», що лежить в основі забезпечення роботи серверу, служб безпеки, маршрутизації, безпеки функціонування організаційній структурі та системи управління.

Мета роботи: удосконалення системи мережі та спостереження дата центру, щоб забезпечити мінімальні енерговитрати з дотриманням вимог протікання технологічного процесу.

В роботі вирішені наступні завдання. Визначити вузли мережі, на які найсильніше впливає інформаційне перевантаження мережі. Визначити умови, та параметри властивостей технічних пристроїв мережі за яких може виникнути витік даних. Розробити рекомендації щодо модернізації мережі для підвищення її стійкості до перевантажень. Визначити найбільш «слабкі» вузли комп'ютерної мережі, які у випадку перевантаження приводять до втрати працездатності мережі і розробити сервер для вирішення такої проблеми.

При її реалізації використані спеціально розроблені моделі серверного і апаратного стеження.

Практичні результати: визначені недоліки і шляхи удосконалення комп'ютерної мережі. Застосовані наукові розробки з моделювання комп'ютерних мереж, серверів управління показали свою достовірність у багатьох прикладах їх застосувань.

СИСТЕМА, КОМП'ЮТЕРНА МЕРЕЖА, НАЛАШТУВАННЯ, МАТЕМАТИЧНА МОДЕЛЬ МЕРЕЖІ, ТЕОРІЯ МАСОВОГО ОБСЛУГОВУВАННЯ, УПРАВЛІННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ЗМІСТ

Вступ.....	10
1 Стан питання і постановка завдання дослідження	13
1.1 Загальна характеристика об'єкта управління	13
1.1.1 Характеристика галузі	12
1.1.2 Аналіз об'єкта впровадження	16
1.3. Аналіз існуючих проблем	20
1.4 Способи обробки і передачі інформації, принципи побудови досліджуваного об'єкта	17
1.5 Мета і завдання дослідження	27
1.6 Визначення напрямків рішення поставлених завдань	24
1.7 Висновки по розділу	25
2 ТЕОРЕТИЧНИЙ РОЗДІЛ	29
2.1 Розрахунок системи контролю роботи відеообладнання з сервером інформації	29
2.2 Аналітичні моделі мереж	34
2.3 Висновки по розділу	34
3 РОЗДІЛ СИНТЕЗУ СИСТЕМИ КОНТРОЛЮ.....	39
3.1 Розробка схеми функціональної структури.....	40
3.2 Аналіз джерел інформації.....	42
3.3 Вибір елементної бази системи.....	43
4 РОЗДІЛ РОЗРОБЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....	43
4.1 Призначення і область застосування програми.....	44
4.2 Обґрунтування технічних характеристик програми.....	45

4.2.1 Постановка завдання на розробку програми	45
4.2.2 Опис алгоритму і функціонування програми	45
4.2.3 Опис і обґрунтування вибору методу організації вхідних та вихідних даних.....	45
4.2.4 Опис і обґрунтування вибору та складу технічних і програмних засобів.....	46
4.3 Опис розробленої програми	47
4.3.1 Загальні відомості.....	48
4.3.2 Функціональне призначення	49
4.3.3 Опис логічної структури	47
4.3.4 Використані технічні засоби	49
4.3.5 Вхідні дані	50
4.3.6 Вихідні дані.....	51
4.4 Очікувані техніко-економічні показники	51
5 ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ	52
5.2 Висновки по розділу	52
ПЕРЕЛІК ПОСИЛАНЬ	53
ДОДАТОК А - ТЕКСТИ ПРОГРАМ НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ	54

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,
СКОРОЧЕНЬ І ТЕРМІНІВ**

КСА НА – комп’ютерна система насосних агрегатів;

СРС – сервер стеження;

ТП – технологічні процеси;

ПО – пульт оператора;

ТВ – телевимірювання;

ВС – виконавчий співробітник;

ПЛК – програмований логічний контролер;

SDK – відкриті мережеві інтерфейси;

VLAN – віртуальна локальна мережа;

DHCP – протокол динамічної настройки вузла;

RS-485 – технологія передачі даних по мережі;

КП – контролюючий пристрій.

ВСТУП

Розвиток інформаційних технологій тісно пов'язаний із потребою населення. Уявлення теперішнього світу без технологій неможливе. Постає питання що до забезпечення захисту важливих вузлів. Щоб забезпечити надійну безпеку - потрібно високо кваліфікаційний персонал та прилади, так як виробництва працюють цілодобово то і охоронна система потрібна як ніколи, але даний дипломний проект спрямований на розробку саме серверної частини яка керує відеоспостереженням, об'єкту «інформаційного центру» де зберігаються всі важливі документи та відеозаписи за широкий період часу.

Ринок систем відеоспостереження дуже великий і складається з безлічі вертикальних галузевих ринків, які перебувають на різних стадіях розвитку. Галузеві ринки, найбільш сприйнятливі до нововведень технологій відеоспостереження - це промислове виробництво, енергетика, транспорт, освіту, а також системи «Безпечного міста». На цих ринках активно впроваджуються новітні мережеві системи відеоспостереження на базі IP-технологій.

За оцінками аналітиків і даними фінансових звітів провідних виробників програмно-апаратних рішень для систем мережевого відеоспостереження цей ринок буде рости із середньорічними темпами понад 10% до 2026 р У 2020 році ринок оцінювався в 45 млрд. дол. і прогнозується його зростання до 75 млрд. дол. до 2025 року.

При проектуванні і побудові систем відеоспостереження одним з основних завдань є вибір станційного устаткування, визначення його характеристик і складу. В IP-відеоспостереження камери можуть мати різний функціонал, кодеки, ступінь компресії, швидкість запису, дозвіл і т.п. Тому правильно вибрати склад і ресурси сервера для IP-відеоспостереження буває непросто.

Метою роботи і завдання дослідження.

Метою представленої роботи є забезпечення ефективного функціонування серверу та системи керування камер

Для досягнення поставленої мети необхідно вирішити такі завдання:

- Вибір платформи
- Ресурси платформи
- Побудова схеми та розрахунку систем
- Вибір типу підключення та серверу
- Опис ПО
- Опис вибору програмного коду

Об'єкт дослідження

- Інформаційна складова серверу та програми

Предмет дослідження

- Склад, параметри, методи, оцінювання серверного обладнання та софту

Методи дослідження

- Серверний та програмний моніторинг і налаштування систем

Ідея роботи

- Обґрунтування структури та параметрів комп'ютерної системи відеоспостереження дата-центру компанії «Датасфера» з детальною розробкою сервера бази даних відеоконтенту

Розраховувати ресурси ПЕОМ треба завжди за максимальними параметрами. Навіть якщо в ТЗ вказано дозвіл менше, ніж передбачено для IP-камер та мережі.

Наукові положення

1. Встановлено, що при збільшенні кількості джерел інформації та збереженні постійного періоду опитування виникає імовірність втрати повідомлень ще до досягнення 100% завантаженості сервера.
2. Встановлено, що використання одного сервера з подвійною потужністю більш виправдане, ніж використання двох серверів з початковою (первинною) потужністю.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

1.1 Загальна характеристика об'єкта управління

1.1.1 Характеристика галузі

На 2020 рік постає питання захисту даних від можливих ураження зі сторони великих дата центрів які накопичують мільйони терабайтів інформації своїх користувачів.

З метою захисту даних на високому рівні потрібно забезпечити інформаційно технологічне рішення по захисту серверних кімнат. Технологічний процес включає всі етапи від розробки до реалізації продукції у сфері захисту серверних кімнат та вузлів підключення безпосередньо до серверів.

Системи відео - спостереження знаходять широке застосування в комплексному захисті об'єктів у державних структурах, правоохоронних органах, службах безпеки банків, комерційних установах, де вони використовуються для контролю доступу, у якості пошукових і оглядових засобів.

На даний момент цифрові системи представляють реальну альтернативу аналоговим і мають переваги в наданих можливостях обробки, запису і передачі (мережних можливостей) відео зображення. Такий перелом зв'язаний у першу чергу, із наступними факторами:

- падінням вартості збереження даних на жорстких дисках та носіях;
- доступність могутніх обчислювальних засобів та передачі даних;
- розвиток програмних засобів, орієнтованих на роботу з відеосигналами.

Сучасні системи в переважній більшості випадків є гібридними. Це означає, що відеосигнал формується ПЗС-матрицею відео-камери в цифровому виді. Далі ця цифрова інформація перетвориться електронікою відеокамери в

аналоговий сигнал, що надалі надходить на пристрій оцифровки, що перетворює його знову в цифрову форму. Оцифрований сигнал можна зберегти на жорсткому диску комп'ютера або передати його через інтерфейсний модуль, наприклад, у мережу Ethernet, наведено на рисунку 1.1

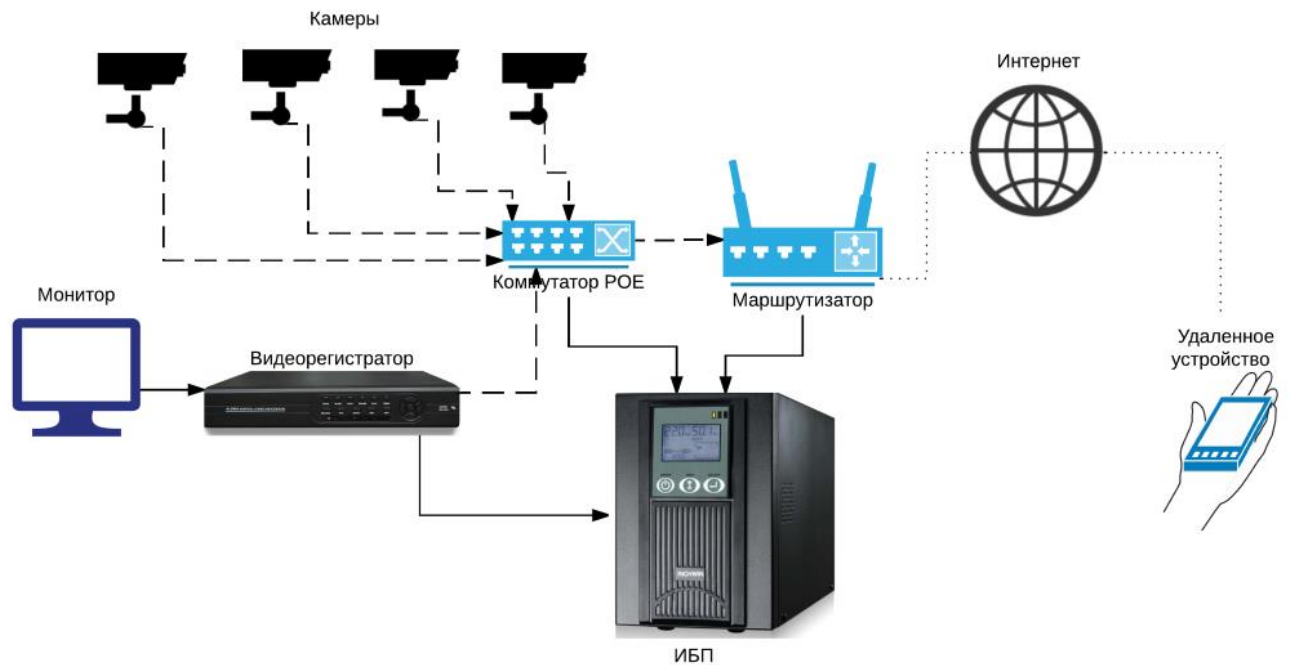


Рисунок 1.1 – Системи запису та передачі сигналів

Існують і цілком цифрові у нашому випадку доцільно застосовувати цілком цифрову систему за для більшої безпеки систем що оперують винятково з відеоданими в цифровій формі. Зокрема, така система може бути побудована на основі IP відеокамери з убудованим WEB-сервером, або цифрової відеокамери і сервера на базі комп'ютера. Такі системи можуть, активізуватися по сигналу тривоги і передавати через мережу відеосигнал з невеликою передісторією на віддалений комп'ютер. Можлива і безупинна передача цифрового відеосигналу від такої системи в мережу. Цифрова техніка грає усе більшу роль. Цифрові системи обробки розділяються на два класи: цифровий відеомагнітофон (NVR,

Network Videorecorder) і комп'ютерна система відеоспостереження. Цифрові системи обробки відео зображення представлені на рисунку 1.2

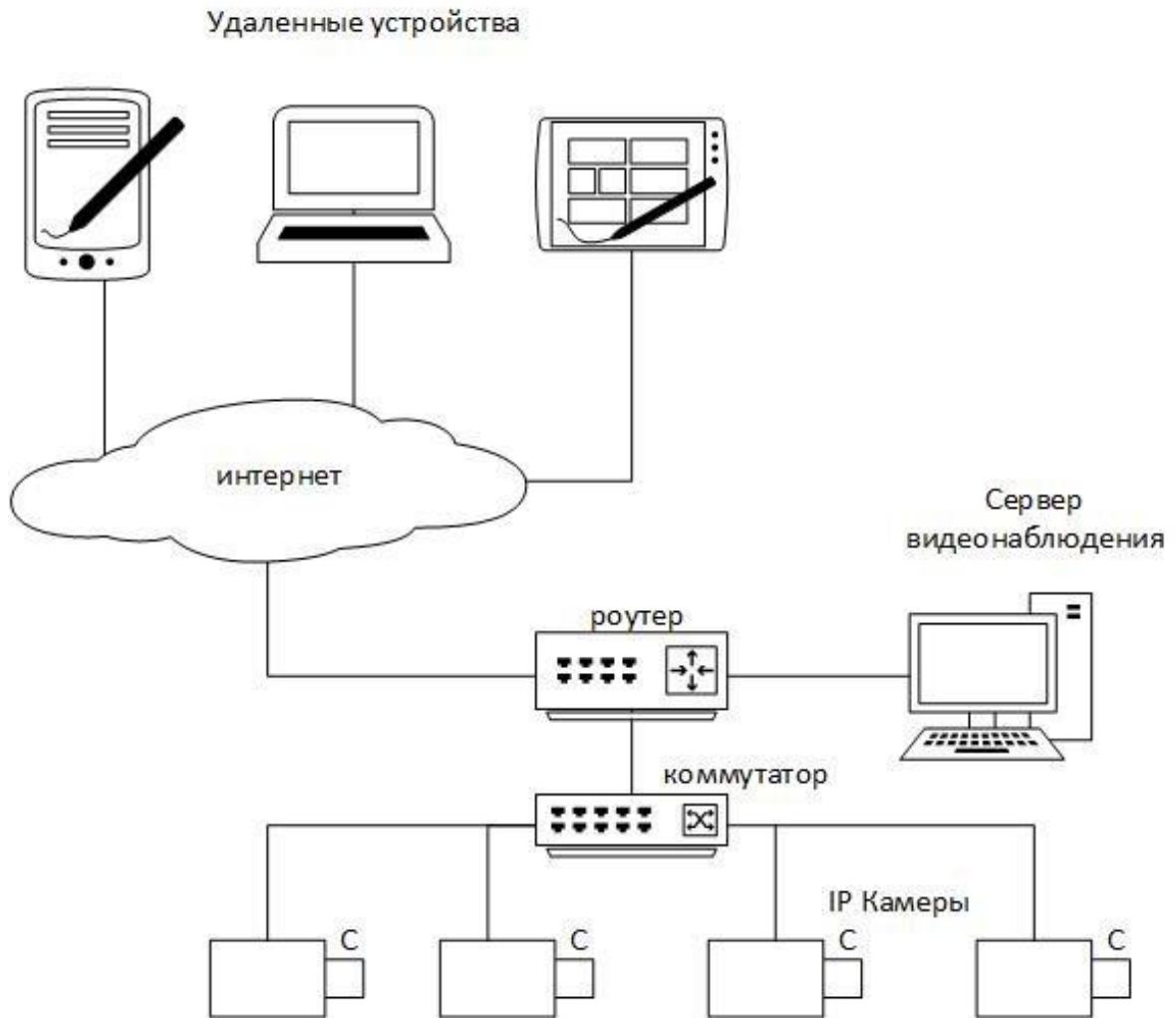


Рисунок 1.2 – Цифрова система обробки відео зображення

Будь-яка цифрова система володіє суттєвими перевагами перед аналоговими системами:

- запис на цифрові носії (жорсткі диски) значно перевершує по якості і надійності будь-які аналогові системи;

- інформація, розміщена на цифрових носіях, не піддана старінню, може багаторазово зчитуватися і вільно копіюватися без погіршення якості;
- швидкість запису, копіювання і стирання інформації істотно перевищує будь-які аналогові системи. Швидкий доступ до будь-якого фрагмента запису спрощує роботу з інформацією;
- передача цифрової інформації. Поза залежністю від використовуваного типу з'єднання (модем, локальна мережа, оптоволоконна і т.д.) якість переданого зображення не зміниться;
- зображення не спотворюється і не втрачає в якості при передачі на будь-які відстані;
- цифрова обробка сигналів. Використання сучасних технологій дозволяє значно розширити спектр додаткових можливостей при роботі з зображенням і звуком;
- детектори руху. Функція дозволяє виявляти наявність будь-яких об'єктів, що переміщуються.

1.1.2 Аналіз об'єкта впровадження

В якості об'єкту виступає серверна кімната дата-центру "Дата сфера". Це приміщення яке включає в себе багато рівнів та має широкий спектр надання безпеки. Тому потребує новітню систему безпеки та відео спостереження. Але новітня система безпеки не дає цілковитого захисту, потрібно враховувати важливі аспекти такі як:

- мертві зони;
- кут нахилу та повороту;
- нормальна температура приміщення;
- швидке на надійне підключення до мережі;
- дистанція між вузлами.

Схема розміщення камер зображена на рисунку 1.3

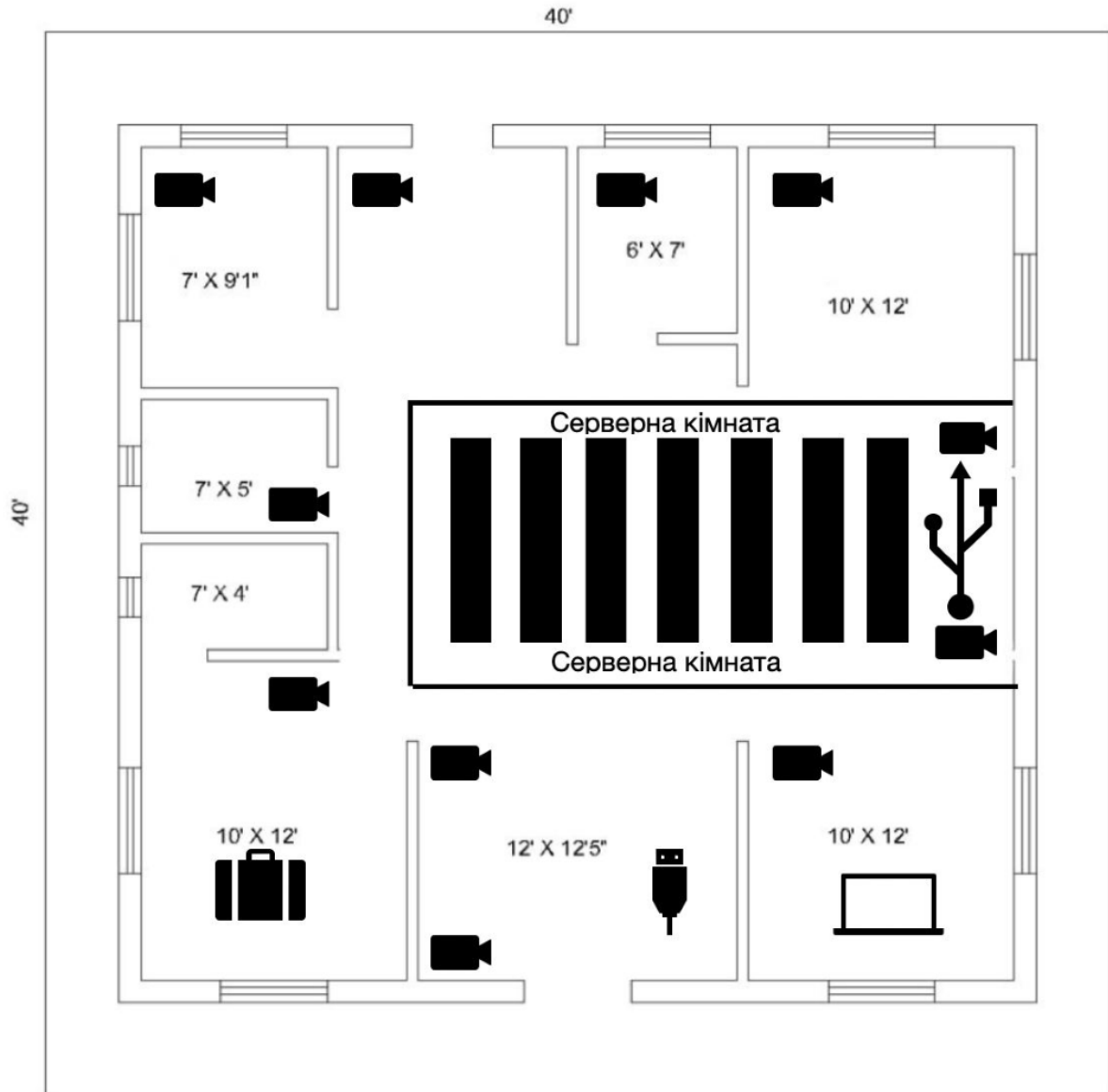


Рисунок 1.3 – Зображення камер на плані будівлі

С урахуванням конкретних умов і особливостей процесів діяльності на об'єкті система відеоспостереження в складі інтегрованої системи безпеки повинна забезпечувати виконання таких функцій:

– пряме відеоспостереження оператором контрольованої зони, виявлення та ідентифікацію суб'єктів спостереження – людей, транспортних засобів, майна, елементів об'єктової інфраструктури;

– передачу візуальної інформації про стан охоронюваних зон, приміщень, периметра і території об'єкта в пункт охорони для відеоверифікації тривоги – підтвердження за допомогою відеоспостереження факту порушення зон охорони та виявлення помилкових спрацьовувань охоронної сигналізації;

– запис відеоінформації в архів для подальшого аналізу стану об'єкту, що охороняється (зони), тривожних ситуацій, ідентифікації порушників та інших завдань.

Відеоспостереження в сучасному світі, в тому числі в Україні, успішно використовується для моніторингу та управління технологічними процесами на виробництві, у сфері серверних послуг та інших. Пристрої обробки та запису - відео реєстратори (NVR), плати відео захвату, відео сервери - дозволяють обробляти потоки відеоінформації, одержувані від кількох відеокамер, аналізувати відео потоки, записувати їх і видавати в заданому форматі на монітор і в локальну або глобальну мережу для віддаленого перегляду. Вони також дозволяють записувати з подальшим відтворенням зображення (як безпосередньо від відеокамери, так і від пристроїв обробки).

Сучасні системи відеоспостереження зазвичай використовують для накопичення і зберігання відеоінформації звичайні накопичувачі на жорстких магнітних дисках (HDD), а при великому обсязі інформації - накопичувачі, об'єднані в RAID.

В якості пристроїв відображення інформації для систем відеоспостереження зараз застосовуються комп'ютерні монітори, а також за допомогою прикладної програми або web-браузера організовується перегляд відеоінформації на моніторі комп'ютера, мобільного телефону. Особливою

популярністю користуються програми для відеоспостереження на базі Android та iOS.

Дуже важливим компонентом будь-якої системи відеоспостереження є середовище передачі сигналу - кабельна мережа, Wi-Fi мережа та підсистема живлення. У нашій системі сигнали передають через Wi-Fi мережу до контролера. Контролер в свою чергу підключено до мережі за допомогою RJ45.

При побудові системи відеоспостереження з використанням IP технологій кабельна система будується за принципами локальної комп'ютерної мережі (LAN) і може використовувати різну фізичну середу для передачі інформації - мідний кабель типу "вита пара", бездротову мережу WiFi etc.

Для живлення відеокамер традиційно може використовуватися силовий кабель, але останнім часом набирають популярність технології POE (power over ethernet), де живлення і дані передаються по одному кабелю типу вита пара. Передача відеосигналу від а HD відеокамери до пристрою обробки традиційно проводиться через мережу Wi-Fi, але найбільш прогресивним є застосування кабелю типу "вита пара" з пристроями передачі відеосигналу по витій парі.

Найчастіше від якості компонентів і застосовуваних матеріалів кабельної мережі і устаткування живлення залежить якість системи відеоспостереження в цілому, оскільки кінцеві пристрої - відеокамери, NVR. Мають дуже хороші параметри - такі як нічне бачення, сигналізація, датчик контролю температури.

Серверна кімната виробляє велику кількість тепла, тому є необхідним встановлення терморегулювання або спеціалізованого термометру, та розробка спеціального програмного забезпечення для нього.

І власне при передачі відеосигналу на відстань і виникають інженерні завдання з побудови якісної системи відеоспостереження у серверній кімнаті, тобто на перший план при проектуванні й реалізації системи відеоспостереження виходить вибір середовища передачі, грамотного розрахунку кабельної або

бездротової мережі з урахуванням постійно зростаючої роздільної здатності відеокамер і пристроїв обробки систем відеоспостереження.

1.3 Аналіз існуючих проблем роботи відео обладнання

Впровадження відеоспостереження в будь-якій організації пов'язане з цілою низкою проблем. Не в останню чергу вони пов'язані з тим, чи знайде архітектор системи правильний баланс між якістю, вартістю та пропускнуою спроможністю. Це завдання стає ще більш складною в певних умовах, наприклад, при необхідності встановити відеоспостереження на нафтовому родовищі, біля вуличних банкоматів, на перехрестях і в інших місцях, де неможливо забезпечити контроль над навколишнім середовищем і які характеризуються підключенням до IP-мереж з обмеженою пропускнуою спроможністю .

Більшість сучасних систем відеоспостереження призначені для роботи в так званих офісних умовах. Але багато хто з сучасних систем відеоспостереження знаходять своє застосування і в далеких куточках земної кулі, вони встановлюються по периметру об'єкту, що охороняється, в важкодоступних і подібних місцях. Вони повинні працювати в умовах екстремальних серверних температур - від -20°C до $+70^{\circ}\text{C}$ - і використовувати мережі з обмеженою пропускнуою спроможністю.

Деякі поширені проблеми:

- білі і різнокольорові лінії на екрані:

Якщо кабелі прокладені поруч з високовольтними джерелами живлення, на відео будуть виникати перешкоди.

- засвічування інфрачервоним випромінюванням:

Світловідбиваючі і великі світлі поверхні є найбільш поширеними причинами виникнення відблисків від ІЧ-підсвічування. Крім того, об'єкти які знаходяться дуже близько до камери, можуть привести до того що на екрані ви будете бачити тільки невиразні білі силуети.

- відеокамери спостереження з ІЧ-підсвічуванням не бачать в темноті:

Інфрачервоні камери як ліхтарики - щоб дозволити нам бачити в темряві, їм потрібна поверхня, від якої промінь світла може відбитися і потрапити в наші очі.

Якщо ви направите ліхтарик в небо, ви нічого не побачите. Те ж відноситься до камер безпеки. Якщо ви встановите відеокамеру спостереження так що ІЧ променям ні від чого буде відображатися, ви нічого не побачите.

- відблиски в денний час:

Відблиски від сонця, промені якого заливають приміщення через скляні двері і вікна, можуть зіпсувати всю картину.

- недостатня потужність:

Однією з найбільш поширених причин несправності систем відеоспостереження є неправильне використання джерел енергії. Камери відеоспостереження споживають різні обсяги електроенергії в залежності від номінальної напруги обладнання. У деяких випадках в специфікаціях вказується енергоспоживання камери без урахування інфрачервоного підсвічування, необхідної для відеоспостереження в умовах низької освітленості. Наприклад, в денний час 8-канальна система відеоспостереження може працювати без збоїв, а в нічний час ви можете раптово втратити зв'язок з кількома камерами. Це означає, що джерелам живлення не вистачило напруги для забезпечення роботи камер з увімкненим ІЧ-підсвічуванням.

- недостатнє охоплення:

Камери відеоспостереження, так само як і будь-яке обладнання, мають свої можливості і обмеження огляду.

Так як у них немає іншого вибору, користувачам доводиться докладати додаткових зусиль щодо захисту критично важливого обладнання для відеоспостереження. При цьому витрачають великі гроші і багато сил на переобладнання звичайних мережевих відеореєстраторів та іншого обладнання, яке не було призначене для роботи в таких умовах. Деякі компанії для захисту

обладнання купують системи вартістю кілька тисяч доларів, забезпечені вентиляторами і обігрівачами.

Що ще більше ускладнює функціонування таких систем, це те, що у віддалених місцях їх мережеві можливості ще більш обмежені. Через ці обмеження мережі, користувачі йдуть на компроміси, в тому числі знижують дозвіл і кадрову частоту, що призводить до того, що відеоматеріали стають непридатними для використання в якості доказів.

Новий підхід, який допоможе вирішити ці проблеми, передбачає використання відкритих, інтелектуальних пристроїв відеоспостереження. IP відеокамери спостереження підключаються таким чином, що відеоматеріали витягуються за допомогою системи управління відео (NVR) тільки на вимогу або в разі виникнення будь-якого інциденту.

Інтелектуальний підхід до відеоспостереження і розподілена архітектура не тільки на 95 відсотків вирішують проблеми з мережею, але і підвищують надійність отримання відео, захищаючи відеозаписи від умов, які можуть вплинути на роботу мережі, наприклад, перевантаження або відключення мережі. Відео продовжує записуватися, навіть якщо в мережі відбуваються збої.

Насправді, в даний час існують захищені системи відеоспостереження, які вже спочатку випускаються в сертифікованих, міцних корпусах і здатні витримувати суворі умови. Пристрої укладені в корпуси, які відповідають міжнародним стандартам і ідеально підходять для ведення запису в екстремальних умовах. Таким чином, спочатку добре продумана система відеоспостереження стане незамінним і максимально ефективним рішенням для захисту цінних активів в екстремальних умовах. На сьогоднішній день можна стверджувати, що можливості таких інтелектуальних рішень для відеоспостереження, в дійсності, практично нескінченні.

1.4 Способи обробки і передачі інформації, принципи побудови досліджуваного об'єкта

Одним з основних пристроїв системи відеоспостереження є – відеокамери.

Камера – прилад для прийому і первинної обробки відеоінформації. Усі сучасні камери будуються на основі напівпровідникових ПЗС-матриць. Світло, що падає на матрицю, перетворюється в електричний сигнал, що потім буде оброблятися. Поверхня ПЗС-матриць складається з безлічі світло чуттєвих комірок - пікселів (від 270 000 до 440000). Чим більше число пікселів, тим виходить більш якісне і чітке зображення. Розмір матриці вимірюється в дюймах і приймає значення: 1", 2/3", 1/2", 1/3", 1/4".

Більшість камер у даний час виробляється на основі матриць фірм «Sony», «Samsung», «Sharp». Камери використовуються з об'єктивами. Об'єктив служить для фокусування зображення на матриці камери. Важливою характеристикою є - кут огляду об'єктива.

У залежності від завдань, що стоять, застосовують об'єктиви з кутом огляду від декількох градусів (для концентрації уваги на віддаленому об'єкті) до 180 градусів (для огляду великої території).

Стандартний кут огляду людського ока 60-70 градусів, тому об'єктиви з широкими кутами огляду вносять істотні перекручування в зображення.

Кут огляду у великій мірі залежить від фокусної відстані.

Чим менше фокусна відстань, тим більше кут огляду об'єктива, і навпаки. У системах телевізійного зображення застосовують об'єктиви з фокусною відстанню від 2,8 мм (об'єктиви з широкими кутами огляду) до 12 мм (вузько спрямовані об'єктиви).

Якщо заздалегідь знати габарити і віддалення об'єкта спостереження, то фокусну відстань можна розрахувати по формулах

$$f = v \cdot \frac{D}{V}, \quad (2.1)$$

$$f = h \cdot \frac{D}{H}, \quad (2.2)$$

Де:

D - відстань до об'єкта;

f - фокусна відстань;

V і H - вертикальний і горизонтальний розміри об'єктива;

v і h - розміри зображення об'єктива на ПЗС - матриці.

Таблиця 2.1 – Зв'язок між фокусною відстанню і кутами огляду об'єктивів

Фокусна відстань, мм	Розмір ПЗС-матриці			
	1/3"	1/2"	2/3"	1"
2,6	92,3	116,5		
3,6	67,0	92,6		
4,5	54,4	73,5		
4,8	53,4	71,1	91,1	
5,5	43,7	60,4	77,4	99,2
6,0	41,0	57,1	74,4	
8,0	30,4	43,1	58,1	
8,5	29,0	41,2	54,7	
11,0	22,8	32,7	44,8	
12,0	20,3	29,5		
12,5	20,2	29,1	39,2	55,5
16,0	15,6	22,5	30,5	
25,0	10,2	14,8	20,2	29,2
36,0	7,3	10,6		
48,0	5,9	8,6		

До складових частин об'єкту належать:

- кодування сигналів Бінарне або Тернарне ;
- Wi-Fi або Ethernet використання;

- датчики руху;
- нічне відеоспостереження;
- синхронізація з поштовою скринькою «Gmail»;
- цілодобова перевірка обладнання;
- функція запису на жорсткий диск;
- доступ з браузеру в адмін-панель;
- система контролю температури;
- система швидкого реагування.

Підключення здійснюється за допомогою «витої пари» або по мережі «WIFI».

Сигнал котрий використовується переважно цифровий, для чіткого відображення картинки. Передача сигналу здійснюється за допомогою як і локальної мережі, так і Ethernet.

Функціонування об'єкту залежить від чіткого розуміння розташування та виконання певних вимог до розміщення та підключення.

Системи IP-відеоспостереження дозволяють вести спостереження за об'єктами з використанням ресурсів Інтернет з будь-якої точки світу.

IP-камера має вбудований веб-сервер, мережевий інтерфейс (Ethernet або Wi-Fi) і підключається безпосередньо до LAN / WAN / Internet мережі. IP-камера на відміну, наприклад, від USB-камери не вимагає під'єднання до комп'ютера напрямку. Все необхідне для отримання відео потоку по мережі інтегровано в IP-камеру, треба просто підключити камеру до мережі.

Перегляд, запис і адміністрування можна здійснювати з будь-якого мережевого комп'ютера. Зображення з IP-камер можна подивитися з будь-якого комп'ютера підключеного до Інтернету, якщо власник мережевої камери надав такі

повноваження. Використовуючи IP-камеру ви можете контролювати серверну кімнату або офіс з будь-якої точки земної кулі.

Користувачі можуть звертатися до мережевої камери за допомогою стандартного web-браузера. Залежно від налаштувань доступ до відео та зображення, отриманому IP-камерою, може бути відкритий усім користувачам мережі або тільки авторизованим користувачам.

Підключення веб інтерфейсу здійснюється у адмін панелі. Камери мають властивість підключення бездротово або через виту пару.

Здатність виводу картинки на монітор у 2 режимах, це через браузер та через HDMI кабель, порт якого знаходиться на приймачеві.

1.5 Мета і завдання дослідження

Метою представленої роботи є забезпечення ефективного функціонування вузлів системи відео спостереження на основі аналізу інформації про роботу технічного та серверного обладнання. Забезпечити максимальну швидкодію серверної частини.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- Аналіз існуючого серверного та відео обладнання дата центру;
- Побудова наглядної схеми комп'ютерної ситеми та серверної мережі;

Вибір принципу розрахунку показників якості роботи комп'ютерної мережі;

– Вибір додаткового обладнання, необхідного для коректного функціонування серверної системи;

– Опис програмного забезпечення для моделювання серверної частини;

– Розробка моделі серверно-комп'ютерної системи контролю ;

– Дослідження розробленої моделі та архітектури системи за наявними потребами.

1.6 Визначення напрямків рішення поставлених завдань

Система відео спостереження дата центру може бути реалізована на вбудованих або піднятих серверах. Пуск, налагодження та локальне керування вузлами може виконуватися за допомогою вбудованого інтерфейсу, або мобільного додатку. Віддалене керування може виконуватися за допомогою реального моніторингу.

Система повинна мати можливість дистанційно, через мережу Інтернет, виконувати наступні функції:

- підтримка доступу до всіх вузлів;
- контроль та управління системою відео спостереження (перегляд в режимі реального часу інформації про сервер та відео вузли, пристрої та несправності систем);
- віддалене налаштування та обслуговування;
- швидке управління системою та швидкий доступ до відповідних вузлів;
- аналіз продуктивності серверного обладнання та відео обладнання.

1.7 Висновки по розділу

У розділі максимально розкрита характеристика галузі та об'єкта дослідження, проаналізовано існуючі проблеми в відео-обладнання датацентру, сформульовано основне положення, мету та завдання дослідження.

2 ТЕОРЕТИЧНИЙ РОЗДІЛ

Вихідними даними при виконанні дослідження є кількість серверів, що зберігають інформацію о роботі відео обладнання, час відгуку вузлами передачі. Стан систем спостереження. Та температурні показники.

Метою дослідження є підвищення якості роботи комп'ютерної системи контролю відео спостереження, розрахунку та моделювання мережі при зміні пропускної здатності вузлів камерних стійок, відображення даних у різних частотних діапазонах .

Призначення дослідження розрахунок показників якості роботи відео системи та контролю серверного обладнання.

2.1 Розрахунок системи контролю роботи відеообладнання з сервером інформації

Для розрахунку показників якості роботи системи відеообладнання розглянемо систему масового обслуговування (NVR) з необмеженою можливістю запису інформації декількома каналами обслуговування. Потік повідомлень між сервером та вузлами, продуктивність/інтенсивність обслуговування сервера та вузлів.

Таким чином в середньому безперервно зайнятий сервер відеоспостереження буде накопичувати інформацію у режимі реального часу. Час виконання повідомлень сервером – випадкова величина, що підпорядковується інформаційному потоку.

Інформаційний потік це стабільний рух інформації, спрямований від джерела інформації до отримувача, визначений функціональними зв'язками між ними. Цей потік можна аналізувати в трьох аспектах: синтаксичному — встановлює формальні правила (параметри) побудови інформаційного потоку, взаємозв'язок між його елементами.



Рисунок 2.1 – Схема інформаційних потоків

У нашому випадку, джерелом виступає камера, приймачем або отримувачем є NVR (Network video recorder), розташування приймача у кімнаті охорони.

Одним з основних пристроїв системи відеоспостереження є – відеокамери.

Камера – прилад для прийому і первинної обробки відеоінформації. Усі сучасні камери будуються на основі напівпровідникових ПЗС-матриць. Світло, що падає на

матрицю, перетворюється в електричний сигнал, що потім буде оброблятися. Поверхня ПЗС-матриць складається з безлічі світло чутливих комірок - пікселів (від 270 000 до 440000). Чим більше число пікселів, тим виходить більш якісне і чітке зображення. Розмір матриці вимірюється в дюймах і приймає значення: 1", 2/3", 1/2", 1/3", 1/4".

Більшість камер у даний час виробляється на основі матриць фірм «Sony», «Samsung», «Sharp». Камери використовуються з об'єктивами. Об'єктив служить для фокусування зображення на матриці камери. Важливою характеристикою є - кут огляду об'єктива.

У залежності від завдань, що стоять, застосовують об'єктиви з кутом огляду від декількох градусів (для концентрації уваги на віддаленому об'єкті) до 180 градусів (для огляду великої території).

Стандартний кут огляду людського ока 60-70 градусів, тому об'єктиви з широкими кутами огляду вносять істотні перекручування в зображення.

Кут огляду у великій мірі залежить від фокусної відстані.

Чим менше фокусна відстань, тим більше кут огляду об'єктива, і навпаки. У системах телевізійного зображення застосовують об'єктиви з фокусною відстанню від 2,8 мм (об'єктиви з широкими кутами огляду) до 12 мм (вузько спрямовані об'єктиви).

Якщо заздалегідь знати габарити і віддалення об'єкта спостереження, то фокусну відстань можна розрахувати по формулах

$$f = v \cdot \frac{D}{V}, \quad (2.1)$$

$$f = h \cdot \frac{D}{H}, \quad (2.2)$$

Де:

D - відстань до об'єкта;

f - фокусна відстань;

V і H - вертикальний і горизонтальний розміри об'єктива;

v і h - розміри зображення об'єктива на ПЗС - матриці.

Для захисту камер в серверній кімнати від несанкціонованого доступу забороняється допуск до налаштувань та обслуговування людей, які не мають на те відповідного дозволу керівництва. Повинен бути забезпечений програмний і апаратний захист від спроб несанкціонованого доступу користувачів до внутрішньої системної інформації. Для захисту інформації від несанкціонованого доступу повинні бути передбачені заходи:

- захист паролем довжиною не менше 10 символів для запуску адмін панелі ;
- відсутність в сервері засобів підключення зовнішніх носіїв;
- при використанні зовнішнього носія підключення його в налаштуваннях завантаження тільки при необхідності;
- зміна паролів не менш ніж одного разу на місяць;
- реєстрація даних про нову зміну і оператора, що працює в системі;
- реєстрація запусків оператором додатків на сервері;
- реєстрація входів оператора в систему;
- зберігання БД на жорсткому диску сервера і неможливість її видалення та копіювання оператором.

Підключення здійснюється за допомогою «витої пари» або по мережі «WIFI».

Сигнал котрий використовується переважно цифровий, для чіткого відображення картинки. Передача сигналу здійснюється за допомогою як і локальної мережі, так і Ethernet.

Функціонування об'єкту залежить від чіткого розуміння розташування та виконання певних вимог до розміщення та підключення.

Системи IP-відеоспостереження дозволяють вести спостереження за об'єктами з використанням ресурсів Інтернет з будь-якої точки світу.

Таблиця 2.3 - Порівняльна характеристика технічних параметрів відеокамер

Модель	Виробник	ПЗС - матриця	Дозволяюча здатність	Чутливість	Об'єктив, мм	Електронний затвор	Габарити, мм	Тип	Ціна, грн
HTC-382	Hi-Sharp (Тайвань)	1/2" (500' 582)	420 тв-ліній	0,1 лк F1,4	змінний	-	38' 36' 55	чорно-біла	900
SSC-M254CE	Sony (Японія)	1/2" (500' 582)	380 тв-ліній	0,3 лк F1,2	змінний	авто 1/10000	64' 54' 150	чорно-біла	2650
WAT-902A	Watec (Японія)	1/2" (537' 597)	420 тв-ліній	0,03 лк F1,2	змінний	1/100000, 1/120	34' 34' 58	чорно-біла	2430
TC-552AX	Burle (США)	1/3" (500' 582)	375 тв-ліній	0,015 лк	змінний	авто 1/100000	140' 64' 53	чорно-біла	1930
BW-273CAX	Samsung (П.Корея)	1/3" (512' 582)	380 тв-ліній	0,2 лк F1,2	змінний	авто 1/50000	62' 62' 150	чорно-біла	1300
WV-BP310	Panasonic (Японія)	1/3" (753' 582)	570 тв-ліній	0,06 лк F1,2	змінний	авто 1/10000	67' 65' 123	чорно-біла	3330
WAT-660	Watec (Японія)	1/4" (537' 597)	380 тв-ліній	0,8 лк F2,0	2.5(75°), 3.8, 6, 3.7	авто 1/100000	29' 29' 16	чорно-біла	1350
VM-912	Samsung (П.Корея)	1/3" (512' 516)	350 тв-ліній	2,0 лк F1,0	змінний	Авто 1/16000	Основа 50' 20	кольорова, моноплатна	1539
VK-C220E	Hitachi (Японія)	1/3" (752' 582)	460 тв-ліній	3 лк F1,4	змінний	авто 1/10000	52' 50' 125	кольорова, цифрова	5400
WV-CP410	Panasonic (Японія)	1/3" (752' 582)	480 тв-ліній	0,9 лк F0.75	змінний	авто 1/15600	67' 55' 123	кольорова, цифрова	6048

IP-камера має вбудований веб-сервер, мережевий інтерфейс (Ethernet або Wi-Fi) і підключається безпосередньо до LAN / WAN / Internet мережі. IP-камера на

відміну, наприклад, від USB-камери не вимагає під'єднання до комп'ютера напряму. Все необхідне для отримання відео потоку по мережі інтегровано в IP-камеру, треба просто підключити камеру до мережі.

Перегляд, запис і адміністрування можна здійснювати з будь-якого мережевого комп'ютера. Зображення з IP-камер можна подивитися з будь-якого комп'ютера підключеного до Інтернету, якщо власник мережевої камери надав такі повноваження. Використовуючи IP-камеру ви можете контролювати серверну кімнату або офіс з будь-якої точки земної кулі.

Користувачі можуть звертатися до мережевої камери за допомогою стандартного web-браузера. Залежно від налаштувань доступ до відео та зображення, отриманому IP-камерою, може бути відкритий усім користувачам мережі або тільки авторизованим користувачам.

Підключення веб інтерфейсу здійснюється у адмін панелі. Камери мають властивість підключення бездротово або через виту пару.

Здатність виводу картинки на монітор у 2 режимах, це через браузер та через HDMI кабель, порт якого знаходиться на приймачеві.

2.3 Висновки по розділу

- Робота системи передачі даних відео зображення до серверу представляється системою масового контролю та експлуатацією.
- Представлені основні показники ефективності роботи системи передачі даних та представлені формули розрахунку при зміні продуктивності сервера.

3 РОЗДІЛ СИНТЕЗУ СИСТЕМИ КОНТРОЛЮ

3.1 Розробка схеми функціональної структури

Система стеження дата центру реалізована на вбудованих серверах компанії (рис. 1.1). Пуск, налагодження локальне та віддалене керування вузлами може виконуватися за допомогою WEB інтерфейсу, або мобільного додатку.

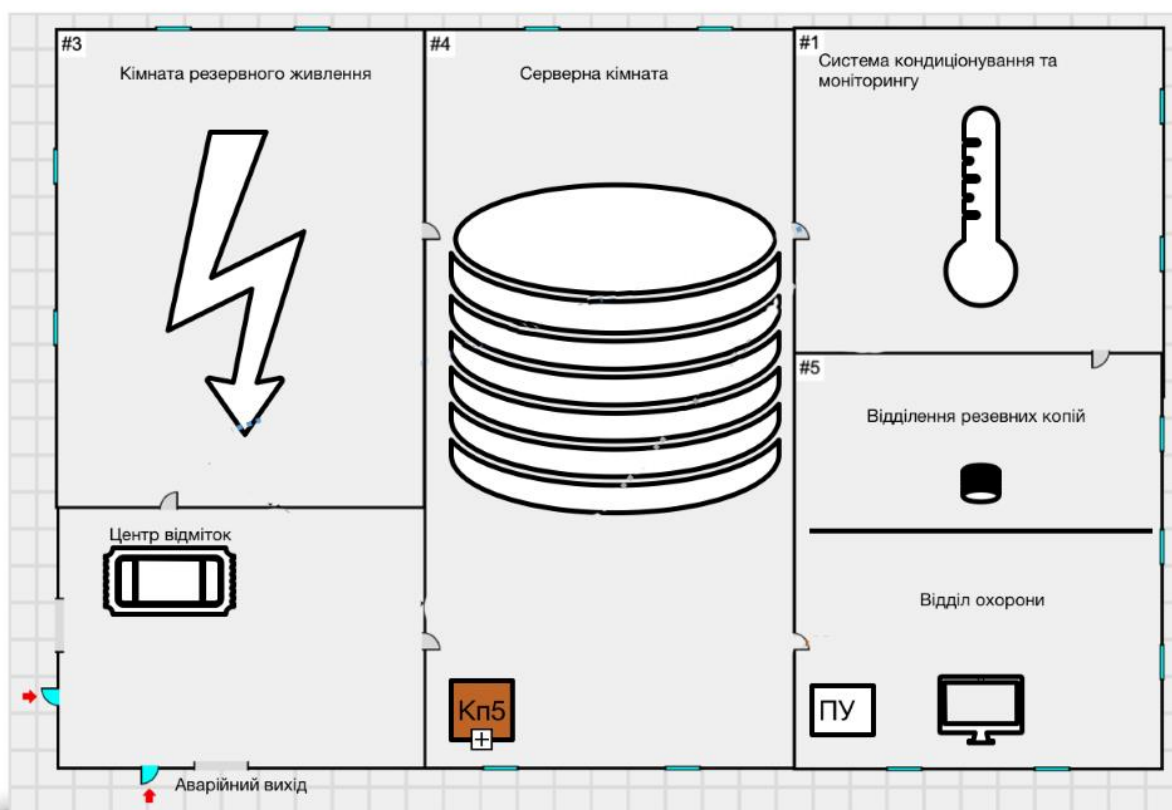


Рисунок 3.1 – Реалізація системи на серверах

Система дає можливість дистанційно, через мережу Інтернет, виконувати наступні функції:

- підтримка доступу до всіх вузлів;
- контроль та управління системою відеоспостереження дата центру перегляд в режимі реального часу;

- віддалене налаштування та корегування системних процесів;
- швидке управління відображенням ;
- аналіз продуктивності та надійності системи.

Зв'язок вузлів виконується за допомогою мережі Ethernet та або оптичних ліній, підключення мережі Інтернет виконується через GPRS/3G/LTE/ROUTER, що дозволяє контролювати параметри системи як локально так і віддалено.

Вузли з'єднуються послідовно в ланцюги за допомогою кабелю вита пара Ethernet з екрануванням групами (до 40 вузлів), два ланцюга під'єднуються до комутаторів (Switch). В свою чергу комутатори Ethernet з'єднуються між собою оптоволоконном. Така схема підвищує надійність системи, та дозволяє зберегти пропускну здатність.

3.2 Аналіз джерел інформації

Відео система контролю безпеки дата центрів повинна виконувати наступні функції: збір інформації; аналіз та обробка інформації; зберігання даних системи; формування відео контенту.

Для виконання вищеперерахованих функцій система повинна мати інформацію про стан та зміни технологічних параметрів серверів та вузлів що відповідають за спроможність безперервного опрацювання .

Джерелами виступають камери Jenpov.

3.3 Вибір елементної бази системи

Виходячи з аналізу схеми функціональної структури дата центру та джерел інформації в ній було вибране наступне обладнання.

Джерелом сигналу впроваджено камери відео-спостереження Jenpov S12WJ20-3-F type F наведені нижче.



Рисунок 3.2 – Камера Jennov type J

Опис камер відео спостереження та їх властивості.

Таблиця 3.1 – Опис камер спостереження jennov

Параметр	Значення параметру
Датчик зображення	CMOS 2,0 мега пікселя (1920 x 1080)
Об'єктив	3.6мм
ІЧ-світлодіоди	59 °36шт ІЧ-світлодіоди по горизонту
Нічне бачення:	100-115 футів
Робоча потужність	DC 12V-1A або мережний кабель
Потужність wifi модулю	До 80 м2
Конструкція кузова	Алюмінієвий сплав
Водонепроникний	IP66, критий і відкритий

Камери мають багатий функціонал від сповіщення детектором руху на електронну пошту до нічного бачення.

До складу камер входять, антена що забезпечує безперебійну передачу даних на великій відстані приблизно до 50 метрів. Камери мають вбудований датчик руху який забезпечує контроль у нічну пору і у денний час. Цілодобовий стримінг навіть у високій якості.

Функція Split Screen за допомогою якої здійснюється відображення декількох зображень на моніторі. Відео менеджер що полегшує контроль над записом який було збережено до жорсткого диску.

Резервна копія відео, функція Video backup дозволяє зробити резервні копії даних, та виконати резервне копіювання даних, як на фізичних пристроях, так і на хмарних та бездротових базах даних.

Підключення камер до приймача, здійснюється через мережу Wi-Fi або виту пару.

Приймач синхронізує камери у мережу за допомогою роздачі ір адрес, через сервіс DHCP, тобто фізичного обмеження на кількість не має, залежність тільки від пропускної здатності та якості пристрою.

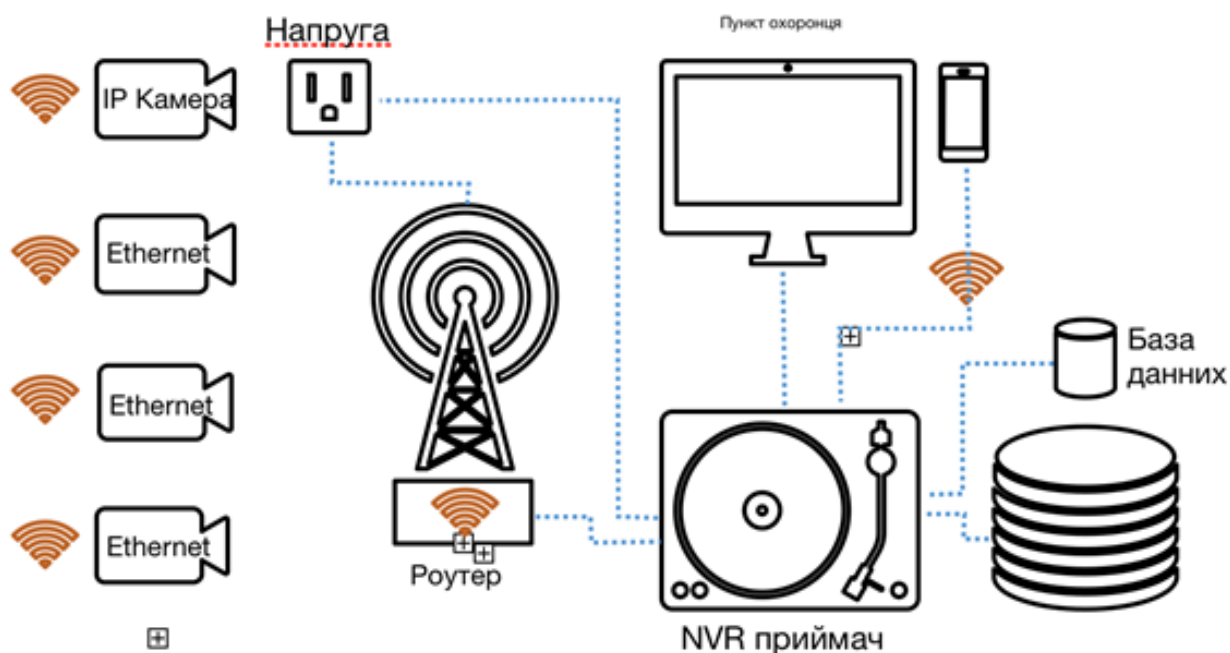


Рисунок 3.3 – Схема підключення системи

В цілому підключення та розташування повинно бути розраховано таким чином щоб забезпечити безперебійну та постійну напругу, безпеку, та оновлення ПО.

Позиційно будова залежить від розташування, роутер повинен мати розміщення у центрі за для певної пропускної здатності. Наступною ланкою системи в цілому є приймач інформації з відеокамер.

Приймач NVR (network video recorder) або відео-рекордер рис 2, головною метою цього пристрою є зчитування інформації з камер, це багато-функціональний приймач що забезпечує також збереження інформації на фізичному носії.

Також було розроблено функцію доступу з мережі до приймача для підвищення мобільності та постійного контролю у дата-центрі.



Рисунок 3.4 – Приймач NVR

Схема портів приймача наведено на рис 3 до них належать порт під антену, WAN port це мережений порт, HDMI під монітор, USB 2.0, та порт для напруги. В таблиці номер 2 наведено опис відео-регістратора.

Таблиця 3.2 - Технічний опис NVR приймача

Параметр	Значення параметру
Вихідна напруга	24В DC
Розміри	124x83x123 мм.
Робоча температура	Від +25 до +70 С °
Потужність	300 Вт
Вхідна напруга	115–230В AC

4 РОЗДІЛ РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1 Призначення і область застосування програми

Для моделювання та виконання правил роботи відео системи по стеженню за роботою дата центру “Дата сфера” в кваліфікаційній роботі розроблено серверно-програмне забезпечення, яке покликано забезпечити надійні та економні результати з реалізацією всіх необхідних функцій.

Серверна частина програми призначена для інсталиювання на персональному комп'ютері з метою забезпечення максимального результату для подальшого безперервного контролю за важливими системними вузлами.

4.2 Обґрунтування технічних характеристик програми

4.2.1 Постановка завдання на розробку програми

Програмне забезпечення серверу контролю роботи відеоспостереження дозволить ефективно реалізувати збір інформації та моніторинг функціонування системи при проведенні досліджень.

Написання програми починається з аналізу роботи системного пристрою на якому буде розміщено сервер та вимог до елементів формування структурної моделі. Процес розробки починається з вивчення вимог до створюваного програмного забезпечення. За розробленою структурною моделлю буде виконана програма.

4.2.2 Опис алгоритму і функціонування програми

Для забезпечення виконання досліджень та збору результатів експериментів для подальшого аналізу параметрів системи контролю в роботі серверу.

Серверна програма завантажується в пристрою вібранного за технічними вимогами .

Встановлюються початкові параметри елементів моделі системи контролю відеостеження. За вимогою правил формується виконувана модель системи контролю.

Після запуску серверу поступово формуються повідомлення, які оброблюються відповідними вузлами моделі. По завершенні формується звіт про виконання експерименту.

4.2.3 Опис і обґрунтування вибору методу організації вхідних та вихідних даних

В роботі розроблена модель системи контролю відеоспостереження.

Для реалізації моделі системи контролю обрано Ubuntu Server 12.04.

Вхідні дані записуються до відповідних секцій програмного забезпечення. Вихідні дані є параметрами, що рахуються програмою при виконанні експерименту.

Вхідні та вихідні дані є потоковими змінними.

4.2.4 Опис і обґрунтування вибору та складу технічних і програмних засобів

У роботі для реалізації моделі контролю роботи відеоспостереження обрано персональний комп'ютер зі встановленим програмним забезпеченням.

Середовище розробки програмного забезпечення Ubuntu Server 12.04 призначене для моделювання. Це програмне забезпечення може використовуватися для вирішення широкого кола завдань.

Програма налаштовується й компілюється в середовищі розробки UNiX ядра на апаратній платформі дозволяє створювати програми великим спектром різних мов програмування.

4.3 Опис розробленої програми

4.3.1 Загальні відомості

Описувана програма є системною реалізацією системи контролю відеоспостереження. Програма компілюється відносно “серверу” обраного для розташування. Програма призначена для виконання експериментальних досліджень відеоспостереження дата центру.

4.3.2 Функціональне призначення

Програма є функціонально завершеною.

Програма призначена для виконання стеження та контролю роботи вузлів датацентру. Програма виконується в середовищі передбаченому ПК.

Програма забезпечує реалізацію наступних функцій системи:

- стеження за вузлами;
- зміну налаштувань серверу обробки ;
- формування потоку повідомлень;
- збереження результатів .

4.3.3 Опис логічної структури

Логічна структура програми представлена у вигляді моделі.

Опис роботи програми:

Встановлюються початкові параметри елементів серверної підсистеми системи контролю відеостеження. За вимогою безпеки дата центру формується виконувана модель системи контролю.

Після запуску виконання моделі поступово формуються повідомлення, які оброблюються відповідними вузлами моделі. По завершенні формується звіт про виконання експерименту.

З аналогією з вивченими готовими системами передбачено два режими поведіння експерименту:

- режим виконання стеження в реальному часі.

-режим виконання в прискореному режимі. Він найбільш оптимальний для виконання декількох послідовних досліджень, які не потребують суттєвої зміни серверних даних.

4.3.4 Використані технічні засоби

Для розробки програми необхідний персональний комп'ютер з наступними технічними характеристиками: процесор 2.0 ГГц і вище, не менше 1024 Мбайт ОЗУ, не менше 1ТБ вільного дискового простору, операційна система Windows 8/8.1/10.

4.3.5 Вхідні дані

Вхідні дані представлені в таблиці 3.4

Таблиця 4.x – Перелік вхідних даних

Вхідні дані	Тип
Кількість потоків	1 потік (залежить від серверу)
Пропускна здатність	До 1 Гбіт/с
Інтенсивність обробки сигналів	1 ms

Продовження таблиці

Вхідні данні	Тип
Аварійний сервер	VDS/VPS
Буфер обміну	сбереження

4.3.6 Вихідні дані

Вихідні дані представлені в таблиці 3.5

Вихідні данні	Тип
Аварійний сервер	VDS/VPS
Кількість пакетів	Від 120 п/с
Кількість втрачених пакетівк	Loss 0

4.4 Очікувані техніко-економічні показники

Данна розробка дозволить на основі аналізу системи даних отриманих при виконанні роботи серверної системи контролю роботи спостереження.

З економічної точки зору, розроблена в роботі моделі системи дозволяє більш раціонально вибирати та використовувати обладнання, і, як наслідок, знизити витрати. Крім того, система дозволить покращити умови стеження та безпеки.

5 ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ

5.1 Розрахунок та моделювання комп'ютерної системи з одним сервером

Розрахунок показників ефективності.

Вихідні дані:

Загальна кількість вузлів контролю – джерел повідомлень. Кількість серверів 1 шт. Інтенсивність надходження повідомлень до сервера у секунду – 30 повідомлень/сек.

Інтенсивність обробки повідомлень сервером – 35 повідомлень/сек.

Сумарну швидкість інформаційних потоків від всіх ІР камер вираховуємо за формулою 222 наведеною нижче

$$B = \sum_{i=1}^n \sum_{j=1}^k V(i, j);$$

5.1

Де :

- B - сумарна швидкість потоків від всіх відеокамер;
- V (i, j) – швидкість j - го «потоків» від i/- ой відеокамери;
- K - загальна кількість «потоків», переданих камерою;
- N - загальна кількість ІР-відеокамер.

Термін «потоків», який використовується в меню ІР- камер для завдання характеристик додатковим потокам і вибору їх кількості.

Від камери йде всього один цифровий потік. При формуванні цього потоку інформація про основний і додаткових «потоків» буде перетворюватися в пакети зі своїми адресами доставки.

І вже ці пакети в загальному інформаційному потоці передаються через мережу.

Для збільшення надійності роботи мережі, в частині запобігання непередбачених перевантажень від зміни інтенсивності руху перед відеокамерами, доцільно значення швидкості потоку збільшити на 25 - 30%

$$V_{max} = 1,3 \cdot V$$

3.2

Вибір пропускної здатності мережі

Пропускна здатність мережі визначається за обраним середовищем передачі сигналу.

Як середовище передачі сигналу використовуються різні види кабелів:

коаксіальний кабель, кабель на основі екранованої і неекранованої витої пари, і оптоволоконний кабель.

Популярним видом середовища передачі даних на невеликі відстані (до 100 м) стає неекранована кручена пара (UTP), яка включена практично в усі сучасні стандарти і технології локальних мереж і забезпечує пропускну здатність до 100 Мбіт / с. Екранована кручена пара (STP категорії 6) дозволяє збільшити пропускну здатність до 1000 Мбіт / с.

Оптоволоконний кабель широко застосовується як для побудови локальних зв'язків, так і для освіти магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох Тбіт / с) і передачу на значні відстані (до декількох десятків кілометрів без проміжного посилення сигналу).

Визначення кількості інформаційних підмереж.

Виходячи з сумарною швидкості інформаційного потоку від всіх IP-відеокамер (V_{max}) обраної пропускної здатності мережі (W), можна визначити кількість інформаційних підмереж, які необхідно створити. Така кількість підмереж забезпечить доставку відео сигналів від відеокамер до сервера без видимих затримок.

$$M = B_{max} / (0,8 \cdot W)$$

5.1

де:

M – кількість підмереж;

B_{max} - сумарна швидкість потоків від всіх відеокамер;

W – пропускна здатність мережі;

0,8 - коефіцієнт, що характеризує максимально допустиму завантаження мережі (80%).

Таблиця 5.1 - Швидкість потоку

Швидкість потоку Мбит/с для кодека H.264				
Камери	Піксель	24к.с	12к.с	6к/с
1.2мп	1280x960	3.78	2.20	1.28
1.9мп	1600x1200	6.03	3.42	1.99
2.1мп	1920x1080	6.51	3.69	2.15
3мп	2048x1536	9.86	5.59	3.24

Мережа побудована на кабелі кручена пара UTP Cat.6, що забезпечує максимальну швидкістю передачі W = 1 Гбіт / с; сумарна швидкість потоку від всіх IP - відеокамер

$$B_{max} = 4 \text{ Гбіт / с};$$

отже, для вирішення завдання доведеться створювати.

$$4 \text{ Гбіт / с} / (0,8 \cdot 1 \text{ Гбіт / с}) = 5/$$

Визначення максимального потоку на один порт, яке здатне забезпечити мережеве обладнання. Вирішення цього завдання має дуже багато варіантів, але, разом з тим, існують основні принципи розподілу потоків і знаходження результуючих швидкостей на ділянках мережі, які ми розглянемо.

Таблиця 5.2 - Швидкість потоку Мбіт/с кодека MJPEG

Швидкість потоку Мбіт/с для кодеку MJPEG				
Розширення	Розмір кадру		Частота кадрі	
Камери	Піксель	24к.с	12к.с	6к.с
1.2мп	1280x960	43.23	21.75	10.92
1.9мп	1600x1200	67.53	33.97	17.05
2.1мп	1920x1080	72.93	36.69	18.41
3мп	2048x1536	110.62	55.64	27.92

При побудові мережі використовується активне обладнання, призначене для поділу / об'єднання потоків і трансляції їх від відеокамери до сервера. Розподіл / об'єднання потоків здійснюють комутатори, які бувають двох типів рис 3.2 – 3.3



Рисунок 5.2 – Простий комутатор



Рисунок 5.3 - Комутатор з комбо портом

Щоб дізнатися максимальний потік на порт на треба зробити наступні кроки зображені на рисунку 3.4 .

Тобто максимальне завантаження порту комутатора визначена в його технічних характеристиках. При завантаженні всіх портів комутатора загальний інформаційний потік не повинен перевищувати значення максимальної пропускної спроможності комутатора. Для виконання цієї умови потрібно визначити максимально допустиму швидкість потоку на кожен порт

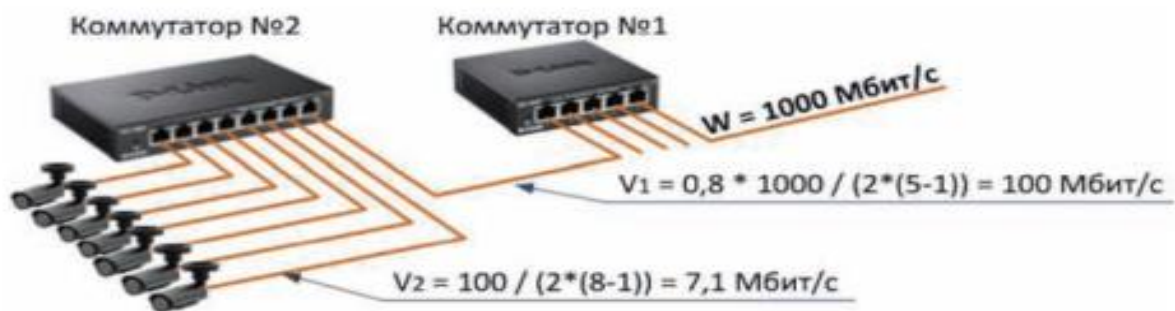


Рисунок 5.4 - Розрахунок максимального потоку на порт

При використанні простого комутатора в мережі, коли до всіх портів крім одного підключені відеокамери, а залишився порт підключений до іншого комутатора (Комутатор No 2, Мал. 5), Максимальний допустимий потік на один порт визначається як :

$$V_2 = V_1 / [2(N - 1)] \quad (5.4)$$

Якщо залишився порт підключений до магістралі (комутатор No 1, Мал. 89898),
То максимальний допустимий потік на порт визначається як:

$$V_1 = 0,8 \cdot W / [2(N - 1)] \quad (5.5)$$

де:

- V_1 (2) - максимальна швидкість для одного порту у комутатора No 1 (2) (Мбіт/с);
- N – загальне кількість портів;
- W - пропускна здатність мережі (Мбіт / с);
- 0,8 - коефіцієнт, що характеризує максимально допустиму завантаження мережі (80%). Якщо задіяти в комутаторі комбо - порт, максимальна швидкість через кожен порт може бути визначена наступним чином:

де:

- V - максимальна швидкість для одного порту (Мбіт / с);
- W - пропускна здатність мережі (Мбіт / с);
- N - загальна кількість портів.

5.2 Висновки по розділу

Розглянуто створення мережі та розрахунки спроможностей сервера. Також розроблена топологія та розрахунки динамічних показників відео системи в умовах цілодобового стеження за датацентром.

Розрахунок показників ефективності виконаного за декількома параметрами, у результаті порівнянь показників моделювання співпадає з граничними показниками для комфортної роботи.

Під часи розрахунку екстремальних показників нагромадження серверу, також сервер приймає динамічне положення, то ж треба розраховувати на підтримку VDS/VPS.

Щоб безперешкодно відповідати гостам датацентру, розрахунок навантажень треба виконувати с запасним простором на враховуючих система.

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи детально розроблено сервер контролю відеоспостереження. Дослідження стану питання, дозволило довести доцільність розробки комп'ютерної системи у дата центрі компанії "Датасфера".

Також, шляхом аналізу характеристик стандартних показників, було сформовано вимогу що до встановлення та розробки відео системи на підприємстві.

На основі обзору технічного процесу комп'ютерної системи у дата центрі було побудовано функціональну та принципову схему розробки, що були використані для розробки програмного забезпечення проектованої комп'ютерної системи.

Таким чином можна зробити висновок що метою кваліфікаційної роботи, детальної розробки серверу спостереження дата центру було виконанно

ПЕРЕЛІК ПОСИЛАНЬ

1. Жуков, І. А. Комп'ютерні мережі та технології : навч. посіб./І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.
2. Груздева Л.М., Монахов Ю.М., Монахов М.Ю. Оценка сетевых характеристик компьютерных сетей в условиях информационного вредоносного воздействия: учебное пособие. / Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2010. – с.
3. Globa L.S. Approaches and technologies of creating data-processing resources in the telecommunication environment – Електроніка і зв'язь. Проблеми електроніки ч.2, Київ, 2005
4. Глоба Л.С. Математичні основи побудови інформаційно телекомунікаційних систем. - К.: Політехніка, 2003. -276с
5. ГОСТ 2.702-75. ЕСКД. Правила выполнения электрических схем. – М.: Госстандарт, 1995. – 115 с.
6. ІР Калькулятор [Електронний ресурс] – Режим доступу : URL : <http://ip-calculator.ru/>. – Загол. з екрана.
7. VLSM Calculator – калькулятор підсетей с маской переменной длины [Електронний ресурс]. – Режим доступу:URL:<http://www.vlsm-calc.net/>. – Загол. з екрана.
8. Вороб'єва Н.И., Корнейчук В.И., Савчук Е.В. Надійність комп'ютерних систем. – К.: «Корнійчук», 2002. – 144 с.
9. Мережеве обладнання [Електронний ресурс] – Режим доступу : URL: https://elmir.ua/routers/router_zyxel_sbg5500-a.html. – Загол. з екрану.
10. Класифікація угроз інформаційної безпеки (Електрон. ресурс)/Спосіб доступу:URL:http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml – Загол. з екрана..

11. 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.
12. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка / Под общей редакцией Ю.В. Новикова. – М.: Эком, 1998. – 288 с.
13. Кулаков Ю.А., Луцкий Г.М. Локальные сети. – К.: Юниор, 1998. – 336 с.

**ДОДАТОК А - ТЕКСТИ ПРОГРАМ НАЛАШТУВАННЯ МЕРЕЖІ
КОМП'ЮТЕРНОЇ СИСТЕМИ**

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ ПРОГРАММИ

Текст програми

804.0220005-01 12 01 =--- ??

Листів

2020

АНОТАЦІЯ

Даний документ містить ПЗ налаштувань та ініціалізації.

Тексти програм реалізовані на мові програмування JavaScript.

```

var f = Flashphoner.getInstance();

f.addListener(WCSEvent.ErrorStatusEvent, errorEvent);
f.addListener(WCSEvent.ConnectionStatusEvent,
connectionStatusListener);f.addListener(WCSEvent.StreamStatusEvent,
streamStatusListener);

//конфигурационный объект
var configuration = new Configuration();
configuration.remoteMediaElementId = 'remoteVideo';
configuration.localMediaElementId = 'localVideo';
configuration.elementIdForSWF = «flashVideoDiv»;
configuration.pathToSWF = «../../dependencies/flash/MediaManager.swf»;

// 'init' для инициализации:
f.init(configuration);

// API ready to start
f.addListener(WCSEvent.StreamStatusEvent, streamStatusListener);
function streamStatusListener(event){
trace(event.status);
}

// configuration API
var configuration = new Configuration();
configuration.remoteMediaElementId = 'remoteVideo';
configuration.localMediaElementId = 'localVideo';
configuration.elementIdForSWF = «flashVideoDiv»;
configuration.pathToSWF = «../../dependencies/flash/MediaManager.swf»;

f.init(configuration);

// initialization

function Flashphoner() {
if (arguments.callee.instance) {
return arguments.callee.instance;
}
arguments.callee.instance = this;

```



```
this.clientVersion = "UNKNOWN_VERSION";
this.clientOSVersion = window.navigator.appVersion;
this.clientBrowserVersion = window.navigator.userAgent;

this.webRtcMediaManager = undefined;
this.webRtcCallSessionId = undefined;
this.flashMediaManager = undefined;
this.swfLoaded = undefined;
this.wsPlayerMediaManager = undefined;
window.AudioContext = window.AudioContext || window.webkitAudioContext;
try {
    this.audioContext = new AudioContext();
} catch(e) {
    console.warn("Failed to create audio context");
}
this.connection = null;
this.configuration = new Configuration();
this.calls = new DataMap();
this.publishStreams = new DataMap();
this.playStreams = new DataMap();
this.messages = {};
this.isOpened = false;
this.listeners = {};
this.roomListeners = {};
this.version = undefined;
this.mediaProviders = new DataMap();
this.intervalId = -1;
this.firefoxCodecReplaicer = {"pcma": "PCMA", "pcmu": "PCMU", "g722":
"G722", "OPUS": "opus", "SHA-256": "sha-256"};
this.firefoxScreenSharingExtensionInstalled = false;
}
```

```
Flashphoner.getInstance = function () {
    return new Flashphoner();
};
```

```
Flashphoner.prototype = {
```

```
    isChrome: function(){
```

```
        return (navigator.userAgent.indexOf("Chrome") > -1) &&
(navigator.userAgent.indexOf("Edge") == -1);
    },
```

```
    isFF: function(){
```

```
        return (navigator.userAgent.indexOf("Mozilla") > -1) &&
(navigator.userAgent.indexOf("Firefox") > -1) && (navigator.userAgent.indexOf("Edge")
== -1);
    },
```

```
    initFlash: function (elementId, pathToSWF) {
```

```
        var me = this;
```

```
        if ( (me.isChrome() || me.isFF()) &&
!me.configuration.forceFlashForWebRTCBrowser ) {
```

```
            //Don't init Flash player for Chrome browser because it has some bugs in
version 46 (Flash no longer detects webcam in Chrome)
```

```
            //Once Flash is not loaded, WebRTC will be used everywhere in Chrome until
the Flash Player bug is not resolved
```

```
//https://productforums.google.com/forum/#!topic/chrome/QjT1GR2IYZM;context-
place=forum/chrome
```

```
        trace("Flash won't be initialized for Chrome");
```

```
        return;
```

```

}

if (typeof swfobject != 'undefined') {
    var params = {};
    params.menu = "true";
    params.swliveconnect = "true";
    params.allowfullscreen = "true";
    params.allowscriptaccess = "always";
    params.bgcolor = (Object.keys(me.configuration.swfParams).length === 0) ?
"000000" : me.configuration.swfParams.bgcolor;
    //in case of Safari wmode should be "window"
    if ((navigator.userAgent.indexOf("Safari") > -1) &&
!(navigator.userAgent.indexOf("Chrome") > -1)) {
        params.wmode = (Object.keys(me.configuration.swfParams).length ===
0) ? "window" : me.configuration.swfParams.wmode;
        //workaround for safari browser, FPNR-403
        swfobject.switchOffAutoHideShow();
    } else if ((navigator.userAgent.indexOf("Mozilla") > -1) &&
(navigator.userAgent.indexOf("Firefox") > -1)) {
        params.wmode = (Object.keys(me.configuration.swfParams).length ===
0) ? "window" : me.configuration.swfParams.wmode;
    } else {
        params.wmode = (Object.keys(me.configuration.swfParams).length ===
0) ? "transparent" : me.configuration.swfParams.wmode;
    }
    var attributes = {};
    var flashvars = {};
    if (swfobject.hasFlashPlayerVersion("11.2")) {
        swfobject.embedSWF(pathToSWF, elementId, "100%", "100%",
"11.2.202", "expressInstall.swf", flashvars, params, attributes, function (e) {
            me.flashMediaManager = e.ref;
            me.swfLoaded = true;
        });
    }
}

```

```
        me.mediaProviders.add(MediaProvider.Flash, me.flashMediaManager);
    });
    } else {
        trace("Problem: Flash not found")
    }
    } else {
        trace("Warning: swfobject.js does not include and flash does not load");
    }
},
```

```
initFlashMediaManager: function () {
    if (isFlashphonerAPILoaded && this.userData) {
        this.flashMediaManager.connect(this.configuration.urlFlashServer,
this.userData, this.configuration);
    }
},
```

```
initWSPlayerMediaManager: function () {
    if (this.userData && this.wsPlayerMediaManager) {
        var config = {};
        config.token = this.userData.authToken;
        config.urlWsServer = this.connection.urlServer;
        config.receiverPath = this.configuration.wsPlayerReceiverPath;
        config.decoderPath = this.configuration.wsPlayerDecoderPath;
        config.videoWidth = this.configuration.videoWidth;
        config.videoHeight = this.configuration.videoHeight;
```

ВІДГУКИ КОНСУЛЬТАНТІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

на кваліфікаційну роботу магістра на тему:

« Обґрунтування структури та параметрів комп'ютерної системи відеоспостереження дата-центру компанії «Датасфера» з детальною розробкою сервера бази даних відеоконтенту »

студента гр. 123М-19-1 Єщенко Станіслава Олександровича

Кваліфікаційна робота представлена пояснювальною запискою об'ємом ____ стор. формату А4 і графічною частиною ____ листів формату А2.

Метою є обґрунтування параметрів системи стеження мережі та серверу .

Мета кваліфікаційної роботи: Удосконалення існуючої системи відеосистеми та серверу шляхом розробки програмної моделі.

Актуальність теми у повному обсязі викладена у вступі роботи. Проведений аналіз характеристик і особливостей відео систем та серверних вузлів. Проаналізовані методи і способи моделювання мереж. Зроблені відповідні висновки що до необхідності аналізу роботи серверу та системи, її стійкості до впливу шкідливого програмного забезпечення на вузли контролю. Відповідно до мети роботи обрані сучасні методи розробки моделі. Для виконання завдань дослідження використовуються методи теорії масового обслуговування, розроблена математична модель комп'ютерної мережі як мережі масового стеження. Проведено дослідження властивостей системи та серверу з різними параметрами інформаційного середовища та апаратних засобів. Науковий підхід до вирішення поставлених у роботі завдань дозволив зробити висновки що до доцільності використання моделей комп'ютерної мережі для формування практичних рекомендацій поліпшення роботи мережі за умови незмінності її структури.

Розроблені моделі серверного ПО та моделі стеження розроблена модель спостереження. Сформульовані критерії якості функціонування об'єкту управління, основним критеріями якості є мінімум витрат електроенергії. На базі безперервної моделі системи управління розроблена цифрова модель системи об'єкта управління.

На базі програмних модулів розроблено ПЗ системи управління для серверу на базі Ubuntu Server що входить до складу, та виконана перевірка функціонування програмного забезпечення. Програмне забезпечення функціонує відповідно до заданих алгоритмів і забезпечує виконання поставлених завдань.

Відповідно до вимог кваліфікаційна робота забезпечена графічними матеріалами.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності фахівця спеціальності 123 «Комп'ютерна інженерія».

Виконані в кваліфікаційній роботі завдання відповідають вимогам до професійної діяльності фахівця освітньо-кваліфікаційного рівня магістра.

Оформлення пояснювальної записки та графічного матеріалу до неї виконано згідно з вимогами. Роботу виконано самостійно, відповідно до завдання та у повному обсязі.

У роботі відзначено такі недоліки:

1. Зустрічаються помилки та неточності у оформленні тексту пояснювальної записки;
2. Не показано результати, які б дозволили повністю розкрити можливості використання математичної моделі комп'ютерної мережі.

Оцінки по розділах - «_____».

Кваліфікаційна робота цілomu заслуговує оцінку «_____95_____».

Керівник роботи

проф. Коротенко Г.М.

09.12.2020 р.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра по темі:

« Обґрунтування структури та параметрів комп'ютерної системи відеоспостереження дата-центру компанії «Датасфера» з детальною розробкою сервера бази даних відеоконтенту »

студента гр. 123М-19-1 Єщенко Станіслава Олександровича

Метою є обґрунтування структури комп'ютерної системи відеоспостереження датацентру.

Висновок про відповідність кваліфікаційної роботи завданню та освітньо-професійній програмі позитивний. У роботі використаний науковий підхід до вирішення поставленої задачі. Відповідно до задач, що вирішувалися, обґрунтовано обрані методи вирішення

Кваліфікаційна робота виконана відповідно до вимог, у повному обсязі. Зміст розділів і підрозділів роботи показують, що здобувач чітко розуміє значення окремих етапів роботи, доцільність глибини розгляду окремих вирішених завдань і необхідності практичного використання результатів. Науковий підхід, використаний у роботі, показує що здобувач володіє сучасними методами математичного моделювання мереж і розуміє доцільність їх використання з практичної точки зору.

Позитивні сторони атестаційної роботи:

1. використано результати аналізу самих сучасних підходів до моделювання вузлів систем спостереження;
2. визначені основні характеристики серверу за математичною моделлю;
3. розроблені моделі постановки вузлів камер спостереження, розроблена модель серверного обладнання, сформульовані критерії якості функціонування об'єкту , основним критерієм якості є мінімум витрат електроенергії та надійність;
4. на базі моделі системи управління розроблена цифрова модель об'єкта управління;

5. на базі програмних модулів розроблено ПЗ системи управління для сервером, та виконана перевірка функціонування програмного забезпечення. Програмне забезпечення функціонує відповідно до заданих алгоритмів і забезпечує виконання поставлених завдань.

Основні недоліки атестаційної роботи:

1. не використані усі можливості розробленої математичної моделі комп'ютерної мережі;
2. значно завищений об'єм пояснювальної записки.

Кваліфікаційна робота в цілому заслуговує оцінку «_____».

Рецензент _____

____.12.2020 г.