МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

СМЕРЕКА Віталій Володимирович

Корпоративне хмарне відеоспостереження на основі моделі SaaS / Enterprises Clouding Video Surveillance Bases on SaaS model

спеціальність: 6.050102 - Комп'ютерна інженерія
освітньо-професійна програма - Комп'ютерні системи та мережі

Випускна кваліфікаційна робота

Виконав: студент групи КСМ-41/1
Смерека Віталій Володимирович
_____

Науковий керівник:
С.І. Возняк
_____

Випускну кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
О. М. Березький

ТЕРНОПІЛЬ - 2019

РЕЗЮМЕ

Дипломний проект містить 86 сторінок пояснюючої записки, 20 рисунків, 12 таблиць, 4 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою дипломного проекту є технічна реалізація системи корпоративного відеоспостереження на основі моделі SaaS.

Розроблено логічну структуру системи відеоспостереження та політику захисту.

Під час технічної реалізації проведено монтаж та налаштування системи відеоспостереження з використанням хмарних технологій. Проведено первинне налаштування відеокамер, реєстратора та мережевого маршрутизатора, а також з допомогою програмного забезпечення управління та моніторингу системи відеоспостереження компанії HikVision проведено налаштування локальної роботи системи, а також за допомогою хмарного сервісу Ezviz забезпечено інтеграцію системи відеоспостереження з іншими корпоративними об’єктами.

Ключові слова: ВІДЕОСПОСТЕРЕЖЕННЯ, РЕЄСТРАТОР, МАРШРУТИЗАТОР, ПЕРЕНАПРАВЛЕННЯ ПОРТІВ, SAAS, ХМАРНИЙ СЕРВІС.

RESUME

The diploma project contains 86 pages of explanatory note, 20 figures, 12 tables, 4 annexes. The volume of graphic material is 2 sheets of A3 format.

The purpose of the diploma project is the technical implementation of the corporate video surveillance system based on the SaaS model.

The logical structure of the video surveillance system and security policy have been developed.

During the technical implementation, the installation and adjustment of the CCTV system using cloud technologies has been carried out. The initial setup of the camcorder, the registrar and the network router was carried out, and with the help of the software of control and monitoring of the video surveillance system of the company HikVision the local operation of the system was made, as well as with the help of the cloud service Ezviz provided the integration of the video surveillance system with other corporate objects.

Keywords: VIDEO SURVEILLANCE, REGISTER, ROUTER, PORT TRANSFERRING, SAAS, CLOUD SERVICE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SaaS – Software as a Service

ПЗЗ – прилад із зарядним зв'язком

LAN – Local Area Network

WAN – Wide Area Network

КМОН – комплементарна структура металл-оксид-напівпровідник

CCTV – Closed Circuit Television

ТВЛ – телевізійні вертикальні лінії

СВС – система відеоспостереження

DSP – Digital Signal Processor

FTP – File Trasfer Protocol

SMTP – Simple Mail Transfer Protocol

VSaaS – Video Surveillance as a Service

NVR – Network Video Recorder

NAS – Network Attached Storage

POE – Power over Ethernet

ВСТУП

Для забезпечення безпеки приватної власності від кримінальних посягань застосовуються три види пристроїв: пристрої виявлення, фізичні перешкоди і служби охорони.

Поряд із сучасних способами виявлення порушників відеоспостереження на відміну від оповіщення та радіолокації має багато переваг. Головними з них є наявність можливості більш точно оцінювати середовище, відсутність помилкового оповіщення і можливість виявляти і більш того фіксувати кримінальні посягання при постійній санкціонованій дії в середовищі охорони.

Початок етапу технічних пристроїв відеоспостереження характеризують з появою маленьких фотоапаратів в першій половині XX століття. Ці фотоапарати застосовувались для прихованого одержання відео даних. Головним недоліком фототехніки є не можливість моніторингу середовища в реальному часі, записувати рух об'єкта відеоспостереження. Базою перших малогабаритних телевізійних камер, які надавали можливість моніторити переміщення в середовищі охорони, були електровакуумні компоненти.

Великим проривом у напрямку охоронного телебачення стало застосування в 80-х роках камер на базі ПЗЗ-матриць, які дозволили ще більше зменшити розміри і покращити надійність функціонуваня відеокамер. Окрім цього, ПЗЗ-камери характеризуються великою чутливістю в інфрачервоному спектрі, що робить можливою спостереження в цілковитій темряві.

Постійне вдосконалення та широке продукування пристроїів для охоронного відеоспостереження призвело до значного застосування даних

систем з ціллю забезпечення охорони підприємств, організацій, установ, а також і об'єктів інфраструктури фізичних осіб.

Модель відеоспостереження в найкомпактнішому вигляді формується з монітора і відеокамери, на які поступає відеоінформація. Проте на сьогоднішній день розвиток індустрії, мережевих технологій і застосування мережі Інтернет дає можливість вивести їх на якісно вищий ступінь. Сучасні системи відеоспостереження характеризуються максимально можливою ефективністю при мінімальни грошових затратах на введення в експлуатацію. Багато в чому, саме базуючись на власній унікальності, відеоспостереження через Інтернет має велику популярністю при формуванні комплексних моделей охорони. Це можна пояснити тим, що при одних і тих же апаратних пристроях можна сформувати, як відеоспостереження за дитиною під час відсутності матері, так і потурбуватися про охорону середовища та даних великої корпоративної інституції.

1 АНАЛІЗ МЕТОДІВ ПОБУДОВИ СИСТЕМ КОРПОРАТИВНОГО ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Огляд основних компонентів системи корпоративного відеоспостереження

На сучасному етапі системи відеоспостереження формуються з аналогових та цифрових камер відеоспостереження, які мають просту конструкцію і незначну вартість. Ці відеокамери є оптичними інструментами, ПЗЗ-матриці яких утворюють відеоінормацію з світлового потоку, що надходить через об'єктив і комлекс лінз і надходить на цю матрицю [1].

Цифрові відеокамери містять блок цифрової обробки сигналу, вмонтований веб-браузер і надають відеозображення, яке можна надсилати у формі цифрових даних по LAN/WAN мережах для систем відеоспостереження. Досить часто застосовуються КМОН-матриці, в яких використовуються польові транзистори з ізольованим каналом з шарами відмінної провідності.

Об'єктиви використовуються у відеокамерах з ціллю покращення дальності її функціонування, покращення технічних характеристик і формування відеокамери до певного середовища функціонування. Для відеоспостереження за об'єктами, що переміщаються, застосовують об'єктиви зі різною фокусною відстанню - трансфокатори. В середовищі з змінною освітленостю використовують об'єктиви з автодіафрагмою. На мініатюрні відеокамери замаскованої моделі відеоспостереження монтують об'єктиви виду Pin-Hole [1].

Для збільшення кута огляду відеокамери і моніторингу за переміщенням об'єктів відеоспостереження, камери монтують на пристрох, що можуть повертатися. Техніка поворотного пристрою переміщує відеокамеру в вертикальному і горизонтальному, і надає можливість

працівнику комплексу відеоспостереження моніторити однієї відеокамерою велике середовище, що підлягає охороні.

В аналогових моделях, щоб надійно керувати камерами, використовуються такі апаратні засоби, як мультиплексори, перемикачі (квадратори) і матричні пристрої.

Перемикач (квадратор) - це засіб, що містить багато входів для відеокамер і надає можливість працівнику при бажанні перемикатися між інформацією на моніторі або записувати картинку з будь-якої відеокамери, або застосувати автоматичне послідовне переключення відеокамер. Характеристики таких засобів обмежені, тому їх використання доцільно лише в простих комплексах відеоспотереження.

Мультиплексор є набагато кращим засобом. Він надає можливість формувати на одному моніторі зображення від багатьох відеокамер і проводити одночасний запис з багатьох джерел відеоданих. На відміну від квадратора мультиплексор доукомплектовується детектором переміщення і має набагато більше характеристик керування відеокамерами.

Матричні модулі це наступний крок в удосконаленні мультиплексорів. Вони застосовуються для функціонування у великих підприємствах, де вмонтовано багато відеокамер і є декілька працівників відеоохорони.

Відеосервер - є спеціалізованим засобом на основі персонального комп'ютера, що застосовується для запису, формування архіву та моніторингу відео- та аудіоархіву. У багатьох ситуаціях відеосервер трансформує аналогові дані з камер відеоспостереження в цифрове представлення і передає їх на жорсткий диск для збереження, транспортування і моніторингу інформації. Такі засоби мають значне використання при формуванні охорони об'єктів інфраструктури, завдяки гнучкому інтерфейсу і наявністю можливості створити необхідний по співвідношенню ціна/якість засіб для керування архівами аудіо- та відеоспостереження. Вони надають можливість згрупувати між собою

цифрові і аналогові моделі відеоспостереження, сформувати інтеграцію з аналоговими CCTV моделями [2].

Засоби запису відеоінформації (відеореєстратори, відеомагнітофони, відеорекордери) застосовуються для запису, формування архіву та наступного показу відеозображень, що передаються як від відеокамер, так і від мультиплексора моделі відеоспостереження.

Відеомонітори CCTV використовуються для цілодобового формування зображень з камер комплексу відеоспостереження. В залежності від умов до охоронної моделі і відеокамер використовуються чорно-білі або кольорові дисплеї відеоспостереження. Дисплей для відеоспостереження у порівнянні із звичайним телевізором формує досить чітку картинку з великою роздільною здатністю. Люмінофор, який застосовується в цих дисплеях, зроблено з метою підвищеної стійкості, тому що картинка може велику кількість годин не змінюватися.

Відеокамера це засіб, що трансформує світлову інформацію в класичний відеосигнал, який в подальшому передається на засоби обробки сигналу (записуючі пристрої, дисплеї і т.д.).

Роздільна задтність (ТВЛ) - характеристика, що показує детальність картинки, одним словом, чим кращий показник роздільної здатності, тим точніше проглядаються малі об’єкти, такі як номер на вивісці або стать людини. Чорно-білі відеокамери широкого розповсюдження мають роздільну здатність 380-420 ТВЛ, підвищеної роздільної здатності – 560-570 ТВЛ, кольорові відеокамери 280-350 ТВЛ, з високою роздільною здатністю до 460 ТВЛ, а з цифровою обробкою відеосигналу (DSP) до 1200 ТВЛ [3].

У таблиці 1.1 надано орієнтовну таблиця відповідності ТВЛ, картинки в пікселях і роздільної здатності аналогічних камер у мегапікселях.

Таблиця 1.1 – Відповідність вимірів роздільної здатності відеокамер

ТВЛ	Пікселі	Мегапікселі
380	640x480	0,3
430	720x576	0,36
480	800x600	0,5
560	933x700	0,65
600	1024x756	0,75
800	1080x960	1,23
1000	1600x1200	1,92

Чутливість (люкс) - найменша ступінь освітленості (в люксах), при якому відеокамера має можливість форувати відеосигнал. Чим ця характеристика менше, тим менше світла потрібно камері для того, щоб сформувати зображення. Для класичних чорно-білих відеокамер вона лежить в межах 0,4 ~ 0,01 люкс, для високочутливих до 0,00015 люкс, для кольорових 0,2 ~ 3 люкс. У таблиці 1.2 подано освітленість об’єктів в залежності від характеристик середовища.

Таблиця 1.2 – Освітленість об’єктів

Умови	Освітленість, люкс
безхмарний, сонячний день	більше 100 000 (кут сонця 55°)
сонячний день, з легкими хмарами	70 000
похмурий день	20 000
рано-вранці	500
Сутінки	4
ясна ніч, повний місяць	0,2
ясна ніч, неповна місяць	0,02
ніч, місяць в хмарах	0,007
ясна, безмісячна ніч	0,001
безмісячна ніч з легкими хмарами	0,0007
темна, хмарна ніч	0,00005
в приміщенні без вікон	100 – 200
добре освітлені приміщення, офіси	200 – 1000

Кут огляду відеокамери - характеристика, який формується на основі фокусної відстані (f) об'єктива і його режимом. Зазвичай ця характеристика визначається в градусах. Широкому куту огляду, у відповідність ставляться малі фокусні відстані (2,8-5,0 mm). Для моніторингу за далекими об'єктами використовують об'єктиви з великою фокусною відстанню (28,0 - 75,0 mm і більш). При формуванні вимог об'єктива слід зауважити, що режим об'єктива повинен бути рівним режиму камери або бути значно більшим від його [4]. У таблиці 1.3 представлено кути огляду відеокамери у порівнянні з фокусною відстаню об’єктива.

Таблиця 1.3 – Кути огляду відеокамери

Фокустна відстань, мм	Кут огляду по горизонталі, град.	Кут огляду по вертикали, град.
2,45	93	74
2,96	86	58
3,6	72	55
4	68	48
6	50	38
8	38	29
12	22	19
16	17	13

Пр наявності об'єктиву з великим кутом огляду, можна сформувати добру панорамну зйомку, але вдалечінь ви будете бачити погано, розмито, вже не зможете преглядати там якісь мініатюрні об’єкти. А при застосуванні дальнофокусних об'єктивів як правило обмежується поле бачення, але ви будете набагато краще преглядати далекі об’єкти (ефект бінокля).

Автодіафрагма – під час доби освітленість на об'єкті охорони та моніторингу, зазвичай, зазнає змін освітленості. Для формування на бажаному ступені об’єму світла на матриці застосовуються вмонтований в відокамеру автоматизований електронний пристрій або об'єктив з автодіафрагмою.

Об'єктиви з автоматизованою діафрагмою формують освітленість матриці на бажаному ступені, переміщуючи значення діагфрагми. Діафрагма об'єктива, у порівнянні із зіницею людських очей, при великій освітленості скорочується, затухаючи світло, а при малій освітленості розкривається. Це надає можливість формувати інформацію від відеокамери з доброю контрастністю, без затемнення або засвічення. У моделях наружного спостереження надають перевагу використовувати об'єктиви з автоматизованою діафрагмою.

Кольорові чи чорно-білі відеокамери? Це запитання потрібно сформуувати спочатку при розробці моделі відеоспостереження. Чорно-білі камери характеризуються досить великою чутливістю та роздільною здатністю, надають можливість моніторити середовище в інфрачервоному (схованому для ока) спектрі, є більш дешевшими по ціні. Головним недоліком чорно-білої камери є те, що не має можливості встановити колір в середовищі. Для прикладу, синій і зелений об’єкт на дисплеї монітора буде сформований, як сірий об’єкт.

Кольорові відеокамери формують більш кращу картинку і це дозволяє визначити об'єкт моніторингу, для прикладу, документи в офісі, банкноти, пристрої, комп’ютерну техніку, об’єкти і т.д. Недоліком є досить велика ціна, та в окремих категорій неможливість формувати хорошу картинку в темну пору доби.

У окремих кольорових відеокамерах є в наявності стан день / ніч, тобто камера при малій освітленості преформатовується на роботу в чорно-білому стані.

При функціонуванні камери в середині об’єкту потрібно врахувати лише те, як вмонтовані камери підходять в інтер'єру кімнати чи залу. Треба сформувати, де камеру потрібно вмонтувати камеру сховано, а де в необхідному декоративному оздобленні. У будь-якій ситуації потрібно

намагатися, щоб вмонтовані відеокамери не спровоковували відволікання працівників від їх функціональних завдань.

Друга сторона, якщо камера буде монтуватись на ззовні. Зовнішнє середовище в українських умовах це значні перепади температури від -40 до +50 градусів, значна вологість, а також змінне освітлення. Також потрібно враховувати і наявність ситуації фізичного втручання в роботу камери камери.

Для усунення впливу несприятливих кліматичних умов ззовні приміщень, що розміщуються за межею функціонування відеокамери, використовуються спеціальний кліматичний захист (термокожух).

Для збереження відеокамери від зовнішнього втручання використовують спеціальний захист, які виробляються з високоміцних металів, з захисним склом. Такий захист може також укомплектовуватися порібними термозасобами.

Можливість використання детектора переміщення або руху є великою перевагою кожної з моделей камер. Детектор переміщення - це програмна система, головною ункцією якої є ідентифікація руху в полі моніторингу камери об'єктів. Детектор переміщення не тільки виявляє рух в полі моніторингу камери, а й формує розміри об'єкта і швидкість його переміщення. У відповідності до цілей відеоспостереження, детектор переміщення ініціалізують з граничною мінімізацією неправильних ідентифікацій (фільтрацією шуму), формують гнучку логіку аналізу спрацювань (тривожний запис, інтеграція з другими охоронним пристроями)[5].

При поступленні інформації про тривогу з одного з давачів перміщення в пам'яті відеокамери записується відео інормація, які передавалась до, після і в час перміщення і направляється у наперед встановленою адресою FTP або SMTP, або номером телефону.

Що доцільно використовувати - сховане або класичне монтування. Для схованого відеоспостереження застосовуються маленька безкорпусні відеокамери з діаметром об'єктива 1-2 мм (ще їх називають pinhole), які можуть вмонтовуватись в вхідних дверях, стінах. Ці камери зовсім не видно для інших відвідувачів і не дозволяють фізичне втручання і можуть бути замасковані під інфрачервоні чи пожежні сернсори. У разі, коли немає потреби сховати процедуру відеоспостереження використовуються класичні корпусні або безкорпусні відеокамери.

За методом трасляції відеосигналу камери моніторингу розділяються на два класи: аналогові і мережеві. Аналогові камери транслюють відеосигнал по коаксіальному кабелю і під’єднуються до моделі спостереження через BNC-роз'єм. Окремі з них мають вбудовані предатчики відеоінформації по витій парі або оптоволокну - це надає можливість траслювати відеосигнал на значні дистанції без використання підсилювачів.

IP-камери не тільки передають відеосигнал, але також здійснюють оцифрування інформації, кодують (в MPEG-4, M-JPEG і т.д.) і здійснюють передачу відеоінформації по LAN / WAN через мережевий канали Ethernet. Оскільки IP-камери відеоспостереження, зазвичай, мають вмонтований веб-сервер, картинка з них може бути трансльована у вікні звичайного веб-браузера (Internet Explorer, Crome тощо) [6].

1.2 Середовища передачі і обробки відеосигналів

Після отримання заряду з ПЗЗ матриці і трансформація його в електричний імпульс, йому потрібно перемістится шляхом від відеокамери до відеосервера. Це перміщення може бути не близьким, так як камери можуть зміщуватися через кілька кілометрів від середовища локації відеозображення. Також треба взяти до уваги і електромагнітні впливи, які

також вливають певною дією на відеосигнал, тому потрібно зважено підійти до вибору засобу транспортування даних від відеокамери до відеосервера.

Кожен вид має свої обмеження щодо використання, які потрібно взяти до уваги при монтуванні схеми розміщення елементів комплексу. Максимальну дистанція між відеосервером і відеокамерами беручи до уваги метод транспортування відеоінформації представлено в таблиці 1.4.

Таблиця 1.4 – Середовища передачі відеосигналу

Тип кабелю	Довжина ліній зв'язку без підсилювача	Додаткове обладнання	Примітки
Коаксіальний кабель	До 300 м	Не використову-ється	Можливість виникнення струмових петель Чутливість до різних наведень Мала довжина ліній зв'язку
Вита пара	До 1800 м	Передавачі і приймачі сигналу по витій парі	Відсутність струмових петель Висока захищеність від перешкод Вартість кабелю і монтажу нижче ніж при використанні коаксіального кабелю
Оптоволокно багатомодове	До 4 км багатомодове	Передавачі і приймачі сигналу по оптоволокну	Відсутність струмових петель. Максимальна захищеність від наведень
Одномодове	До 40 км одномодове	Передавачі і приймачі сигналу	Відсутність струмових петель. Низька захищеність від перешкод Легкість монтажу

Коаксіальний кабель - найбільш розповсюдженіший метод транпортування зображення в звичайних СВС.

Головними технічними властивостями кабелю є його діаметр, хвильовий опір і погонне затухання інформаційного сигналу.

Зазвичай, вхідний і вихідний опір головних елементів СВС має значення 75 Ом, тобто розраховані на використання кабелів з хвильовим опором 75 Ом. Звідси, використовувати для транспортування відеосигналу кабелі з хвильовим опором, що відрізняється від 75 Ом, не вважається доцільним [7].

Найбільша дистанція транспортування відеосигналу по коаксіальному кабелю впливає від цільових функцій відеоконтролю і встановлюється виходячи з достатнього в межах норм затухання відеосигналу в кабелі (для визначення - 3 дБ, для відслідковування - 6 дБ).

Затухання в коаксіальному кабелі здійснюється в залежності від його розміру і визначається 2,6 дБ на 100 м (для кабелю розміром 6 мм) і 1,4 дБ на 100 м (для кабелю розміром 9 мм).

Беручи до уваги наведену інформацію, можна обрахувати максимальну дальність транспортування відеоінформації по коаксіальному кабелю.

Якщо потрібно передати сигнал на значні дистанції використовуються відеопідсилювачі. При їх застосуванні найбільша дистанція транспортування відеоінформації може бути встановлена за формулою:

$$D_{\max} = 100 \times \frac{K_{\text{п}}}{K_{\text{зат}}}, \qquad (1.1)$$

де $K_{\text{п}}$ - коефіцієнт компенсації підсилювача, дБ;

$K_{\text{зат}}$ - затухання в кабелі на 100 м, дБ.

При виборі і монтуванні коаксіального кабелю, що використовується в СВС потрібно врахувати наступні особливості:

- обирати коаксіальний кабель з двойним екрануванням, що дозволяє забезпечити ступінь уникнення завад не менше 60 дБ;

- використовувати підходи, які мінімізують вплив завад, що можуть виникнути на об'єкті охорони (уникнення або мінімізація іскроутворення, використання в пристроях спеціальних фільтрів для уникнення паразитного високочастотного випромінювання, усунення завад електричної мережі (50 Гц), екранування пристроїв та ін.);

- монтувати кабелі в залах в декоративних трубах, коробах, а в небезпечних (з точки зору фізичного доступу) середовищах - в металевих

трубах і металевих коробах. Також можливе монтування кабелю по вже наявних кабельних шляхах;

- монтувати кабелі ззовні приміщень в грунті або по стінах будинків. Для цього потрібно використовувати спеціальні кабелі в броньованьому корпусі, що повині працювати у випадку значних коливань температур (від мінус 40 до плюс 70 ° С) та високої вологісті (100%), а також витримувати вплив солі, гризунів і сонячного світла. Допускається використання класичних кабелів, що монтуються в герметичних металевих трубках і металевих коробах.

Для транспортування відеоінформації на занчні відстані (до 1,5 км) можливе використання каналу транспортування "вита пара" з конкретними пристроями (передавачем і приймачем) для трансформації відеоінформації в симетричний, тому що на виході відеокамери сигнал несиметричний.

На сьогодні застосовуються чотири підходи транспортування інформації по цифровим і звичайним телефонним каналам:

- підхід з стисканням картинки за принципом "умовного поновлення" (CR);

- підхід для транспортування тільки даних про зміну картинки від кадру до кадру;

- підхід з MPEG-стисканням, в яких застосовуються спеціальні алгоритми стиснення даних про об'єкти, що переміщуються;

- підхід з GPEG-стисканням, які формують незалежну компресію кадру зображення.

У окремих СВС, коли необхідна найвища завадозахищеність, конфіденційність даних і висока якість відеосигналу, використовують волоконно-оптичні канали передачі даних. Довжина таких СВС (як і при транспортуванні по телефонних каналах) практично не обмежується. Значна вартість таких систем обгрунтовується тим, що відеокамери не мають портів для підєднання оптоволоконного кабелю, тому необхідно використовувати в

СВС перетворювачі електричного сигналу в оптичний і назад.Також, прокладання, з’єднання і приєднання оптоволоконного кабелю достатньо важкий процес. Проте при зростанні відстані траспортування відеоінформації кошторис СВС з волоконно-оптичним зв’язком менше кошторису системи транспортування з використанням коаксіального кабелю (через значну кількість коректорів, підсилювачів та інших пристроїв та кабелів). Як приклад, відеоінформація від десятка відеокамер можна траспортувати по одному оптоволоконному кабелю, а у випадку застосування коаксіального кабелю потрібно застосовувати 10 ділянок такого кабелю потрібної довжини і таку ж кількість коректорів, підсилювачів тощо.

При розробці мобільних і переносних комплексів, а також при неможливості або недоцільності використання кабельних каналів застосовують радіоканали для передачі даних. Відстань для передачі при цьому визначається від сотень метрів до декалькох кілометрів. У звичайній ситуації відеокамери приєднують до радіопередавача гігагерцового діапазону. Проте, такі комплекси мають значні недоліки: вони можуть формувати завади для побутового теле- і радіомовлення, а інформацію в середовищі дії передавача може прехопити будь-яка людина.

Багато бездротових систем транспортування відеоінформації має досить мінімальні діаграми направленості. Тому, такі системи критичні до вирівнювання та монтування приймальних і передавальних антен. При розробці таких систем і їх монтуванні головна увага повинна бути зосереджена на способи вирівнювання і стійкості монтування антен. Природні коливання високих будівель, на яких монтуються антени, можуть значно впливати на якість системи транспортування сигналу.

1.3 Організація системи відеоспостереження через Інтернет

Комплекси відеоспостереження, які під’єднані до всесвітньої мережі Інтернет, надають можливість огляду картинки з камер відеоспостереження, які під’єднані до комплексу, з різних куточків планети. Відеоспостереження через Інтернет надає можливість проводити візуальний моніторинг без наявної особистої присутності.

Якщо ваша інфрастуктура не надає доступ Ethernet, то зазвичай Вам потрібно буде використати наступні засоби:

– широкосмуговий модем для приєднання з асиметричним цифровим абонентським каналом (класично надається вашим постачальником інтернет-сервісу) або кабельним телебаченням;

– широкосмуговий маршрутизатор, що також називають Інтернет-шлюзом. Широкосмуговий маршрутизатор надає можливість абонентам локальної мережі разом під’єднуватися до одного каналу до Інтернету. Він також послуговує як інтерфейс між провайдером, Інтернетом і локальною мережею;

– світч, який надає можливість багатьом апаратним засобам з мережі комунікувати напряму один з одним і дозволяє пристосуванням з локальної мережі мати визначені IP-адреси.

Оскільки широкосмуговий маршрутизатор по класичній схемі встановлює автоматичні, локальні адреси IP для елементів з локальної мережі, такі адреси IP можуть бути змінені в процесі роботи. Статична (постійна) IP-адреса повинна використовуватися для мережевої відеокамери. Щоб встановити статичну IP-адресу, необхідно визначити діапазон IP-адрес маршрутизатора, який, для прикладу, може змінюватися від 192.168.0.2 до 192.168.0.35. Якщо потрібно застосовувати IP-адресу в межах дії, типу 192.168.0.150, як статичну адресу IP для відеокамери, можливо, що не потрібно вигадувати, що новий апаратний засіб буде мати конфлікт з іншими засобами, які ідентифікуватимуться через автоматичні адреси.

Встановлення адреси IP для вашої відеокамери може бути здійснена кількома способами, як визначено в налаштуваннях відеокамери. Щойно адреса IP визначена, ініціалізується підмережа, і шлюз (ці дані можуть бути одержані з маршрутизатора), потрібно визначити характеристики налаштування відеокамер: визначені абоненти для формування кола доступу до відеокамери, їхні паролі (рисунок 1.1).

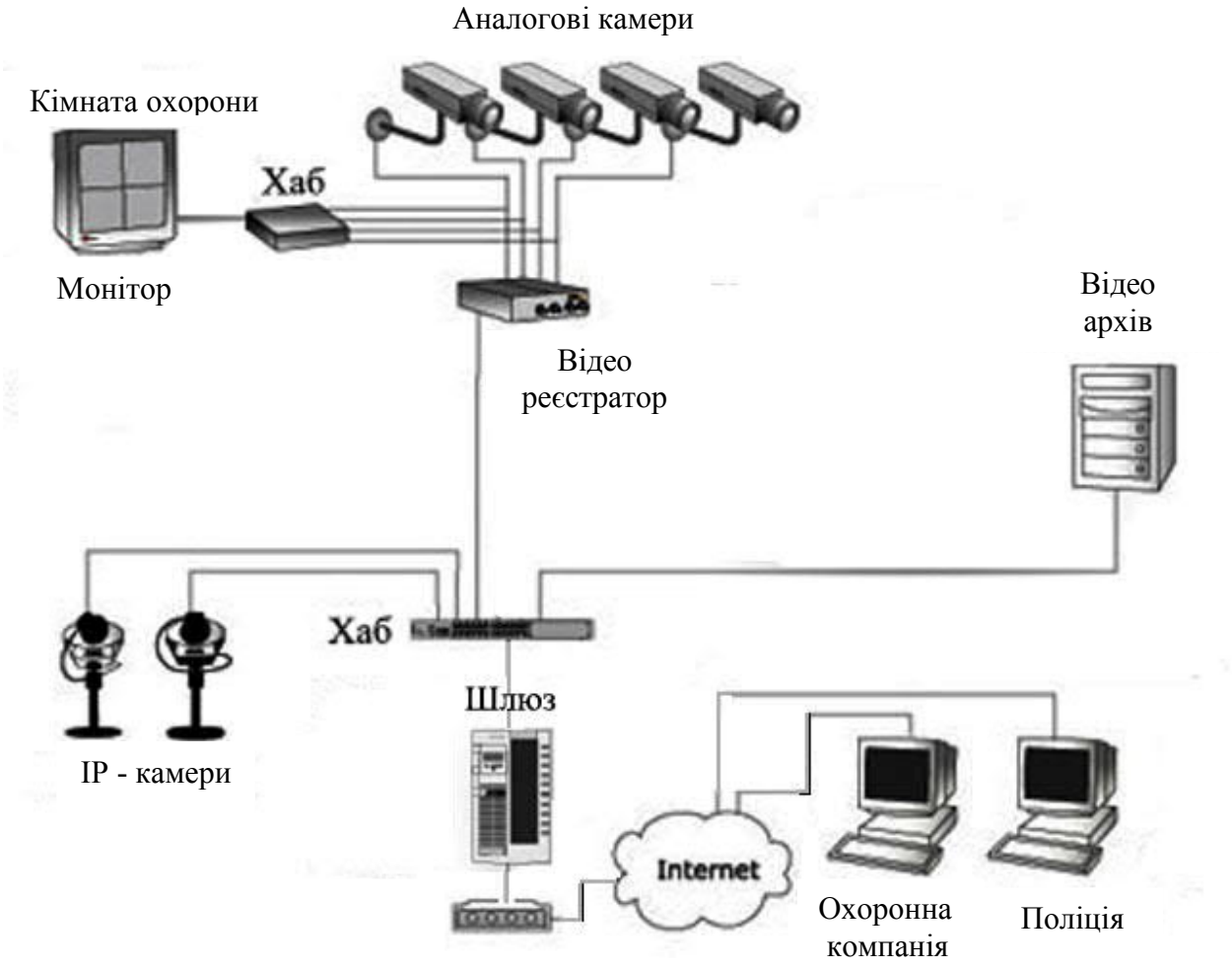

Рисунок 1.1 – Підключення систем відеоспостереження

Також, компанії-виробники пропонують спеціальне програмне забезпечення для відеокамер, які істотно зменшують складність процедури визначення IP-адреси, завдяки вмонтованому програмному забезпеченню для FTP-клієнта, e-mail клієнта, web-сервера, FTP-сервера та ін. Відеокамера

приєднується напряму до LAN/WAN/Internet, аналогові відеокамери приєднуються через відео-сервер - і функціонують в ній як окремий мережевий засіб. Такий підхід відрізняє IP-камери від класичних комп'ютерних відеокамер, які потребують обов'язкового підєднання до персонального комп'ютера через USB порт. Також, IP-камери можуть застосовувати функціонування з одними і тими ж скриптами і JAVA-апплетами.

Широкосмуговий маршрутизатор, як було сказано вище, формує інтерфейс між провайдером, Інтернетом і локальної мережею. Маршрутизатор ініціалізується через зовнішню адресу IP від постачальника інтернет-сервісу та забезпечує внутрішні (локальні) IP-адреси для компонентів у локальній мережі.

Щоб одержати доступ до мережевої відеокамери, що на постійній основі встановлена в локальну мережу, необхідно визначити зовнішню адресу IP вашого маршрутизатора, і налагодити маршрутизатор так, щоб зовнішня адреса IP був перенаправлена до статичної, локальної IP-адреси мережевої відеокамери. Цей процес визначають як перенаправлення порту; тобто, коли використовується зовнішня адресу IP маршрутизатора з будь-якого мережевого пристрою, Інтернет вставлює місцезнаходження вашого маршрутизатора, а він в свою чергу надсилає ваш запит до локальної адреси IP, яка визначена для мережевої відеокамери.

Якщо необхідно сформувати доступ через Інтернет для більше ніж однієї мережево камери, то застосовуються додаткові (unofficial) порти маршрутизатора, наприклад, 80xx і ці потри дозволяють під’єднуватися з мережевою адресою IP відеокамери.

2 ПРОЕКТУВАННЯ КОРПОРАТИВНОГО ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ SAAS МОДЕЛІ

2.1 Хмарний сервіс SaaS для корпоративного відеоспостереження

IaaS, PaaS або SaaS - це моделі надання хмарних сервісів[8]. Те, як вони співвідносяться один з одним, часто зображують у вигляді піраміди з різним рівнем контролю інформації (рисунок 2.1). Вершина - це кінцевий користувач, який працює з особистими даними, «загорнутими» у вигляді програми або сервісу з зручним інтерфейсом. Програма або сервіс розгортаються на якійсь технологічній платформі, це другий рівень піраміди. Нарешті, її основа - це інфраструктура: віртуальні сервери, обчислювальні потужності, накопичувачі і канали зв'язку.

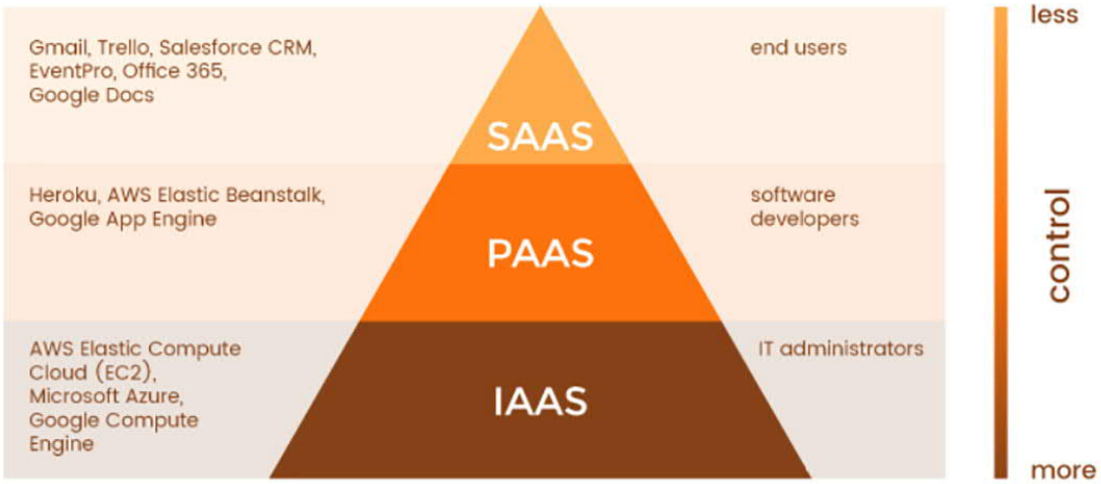

Рисунок 2.1 – Піраміда хмарних сервісів

SaaS (Software-as-a-Service). Ця хмарна модель - найпоширеніша. Програми та сервіси розробляє і обслуговує провайдер, розміщує їх в хмарі і

пропонує кінцевому користувачеві через браузер або додаток на його ПК. Клієнт лише вносить абонплату (або користується сервісом безкоштовно), оновленням і технічною підтримкою програм займається провайдер. SaaS-сервіси можуть надавати місце для зберігання файлів (Dropbox), офісний пакет документів для роботи (Google Doc, Microsoft Office 365), допомагати організовувати фотографії (Flickr) або спілкуватися з іншими людьми (Facebook). Основний клієнт SaaS-сервісів - звичайний користувач.

PaaS (Platform-as-a-Service). В цьому випадку хмарний провайдер надає доступ до операційних систем, засобів розробки і тестування, систем управління базами даних. Провайдер контролює не тільки сервери, системи зберігання даних і обчислювальні потужності, але також пропонує користувачеві на вибір певні платформи і засоби управління ними. Приклади PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry. Користувачі PaaS-сервісів - це розробники ПЗ.

IaaS (Infrastructure-as-a-Service). При цій моделі споживач отримує інформаційно-технологічні ресурси - віртуальні сервери з певною обчислювальною потужністю та обсягами пам'яті. Всім «залізом» займається провайдер. Він встановлює на нього Пз для створення віртуальних машин, але не займається установкою і підтримкою ПЗ користувача. Провайдер контролює тільки фізичну та віртуальну інфраструктуру. Приклади IaaS: IBM Softlayer, Hetzner Cloud, Microsoft Azure, Amazon EC2, GigaCloud. Клієнти IaaS - це системні адміністратори компаній.

З точки зору кінцевого користувача SaaS - сама зрозуміла і зручна хмарна модель. Часто простіше і ефективніше використовувати готовий SaaS-сервіс, який вже відповідає певним вимогам. Але готові рішення не завжди існують, і в такому випадку моделі PaaS і IaaS - незамінні.

Хмарне відеоспостереження (VSaaS) одна з найбільш перспективних технологій поряд з відео аналітикою[9]. Рідкісний експерт не оголосить

відеоаналітика і хмарне відеоспостереження «The Next Big Thing» систем відеоспостереження.

Світовий ринок VSaaS в 2015 році досяг рівня 789,5 мільйонів доларів за даними доповіді IHS, що від загального обсягу ринку відеоспостереження становить приблизно 5%.

Незважаючи на такий скромний результат, на цей ринок, тим або іншим способом, виходять майже всі найбільші світові виробники систем відеоспостереження.

Наскільки великі очікування від ринку хмарного відеоспостереження можна зрозуміти подивившись на одну угоду. Google, через свою дочірню компанію Nest Labs, придбала в 2014 році компанію Dropcam, яка спеціалізується на хмарному відеоспостереження, сума угоди - 555 мільйонів доларів США. Це при тому що в 2014 році світовий ринок VSaaS становив 680 млн доларів США даними IHS [9]. Обсяг світового ринку VSaaS росте зі швидкістю 22% щорічно і до 2022 року досягне $ 6 млрд.

Термін CCTV (Closed Circuit TeleVision) традиційно вважається синонімом украънського терміну - систем відеоспостереження, і дослівно перекладається як - система телебачення замкнутого контуру.

Саме хмарне відеоспостереження розриває цей контур, і розширює коло завдань, які дозволяє вирішувати відеоспостереження. Мабуть, годі й шукати галузі, в якій дистанційний моніторинг читай хмарне відеоспостереження не знайшло б належного застосування.

Промисловим підприємствам потрібно відстежувати роботу обладнання, технологічних процесів, безпеку і якість праці. Торгівля, тут відеоспостереження може використовуватися дуже широко: від мерчандайзингу до бізнес аналітики магазинів. Будівництво, затребувана як охоронна функція відеоспостереження, так і можливості контролю технологічних операцій, віддалений моніторинг ходу будівництва. Транспорт, великий потенціал укладений у вирішенні завдань логістики.

Важливий аспект також полягає в тому, що ви можете моніторити об'єкти відеоспостереження, як із спеціально створеного моніторингового центру, так і зі свого смартфона. Як силами своїх співробітників, так і силами своїх клієнтів, наприклад даючи доступ до камер на своєму сайті.

Хмарне відеоспостереження - це будь-які системи відеоспостереження, що використовують хмарну інфраструктуру в першу чергу для одержання віддаленого доступу до онлайн перегляду, до відеоархіву.

Можна виділити 4 основні сценарії використання хмарної інфраструктури.

1) Доступ до онлайн перегляду і відеоархіву на SD карті камери.

Ви можете використовувати як тільки можливість онлайн перегляду відео з камери відеоспостереження, так і можливість запису і перегляду відеоархіву з SD карти. SD карти як правило в комплекті не йдуть і купуються окремо.

Основними перевагами такого підходу є найнижча вартість, сама висока швидкість розгортання, великий вибір обладнання від провідних світових виробників, мінімальна і легка настройка.

Серед недоліків можна виділити те, що відеоархів може бути втрачений, тому що SD карта легко витягається з відеокамери, в тому числі і зловмисниками. Невеликий розмір відеоархіву. Низький термін служби SD карт.

2) Доступ до онлайн перегляду і відеоархіву на NVR, NAS, сервері.

При цьому підході є можливість онлайн перегляду відео з камер відеоспостереження, плюс можливість перегляду відеоархіву.

Відеоархів в даному випадку знаходиться в локальному відеосховищі тобто в одній локальній мережі з камерами відеоспостереження. В одному програмному додатку ви можете отримати доступ до мережі територіально розподілених систем відеоспостереження.

До перваг такого підходу варто віднести:

– великий вибір обладнання від провідних світових виробників, а значить і найкраща з можливих територіальна представленість є однією з переваг;

– велика ємність відеоархіву, при цьому доступ до відеоархіву надається у вигляді професійного програмного інтерфейсу.

Окремим пунктом варто відзначити, що хмарні сервіси підтримують не тільки відеореєстратори для IP камер (NVR), але і гібридні, HD-TVI, HD-CVI і AHD відеореєстратори, що дозволить використовувати камери практично будь-яких форматів, що в свою чергу сильно позначається на вартості системи відеонагляду. Мережеві сховища підтримують роботу з усіма великими і не дуже виробниками IP камер. В результаті практично повна свобода у виборі відеокамер.

До недоліків слід віднести те, що відеореєстратор, а значить і відеоархів може бути втрачений, в наслідок недбалого поводження або дій зловмисників, висока ціна на спеціалізовані жорсткі диски для відеоспостереження.

3) Доступ до онлайн перегляду і відеоархіву в дата-центрі (хостинг відео).

В даному випадку ми можемо як взагалі обійтися без пристрою зберігання відеоархіву, тобто відео можемо писати безпосередньо в хмару, так і писати відеоархів на локальний пристрій (відеореєстратор, NAS, сервер), і з локального пристрою відправляти в дата центр. У всіх випадках для перегляду відеоархіву ми будемо звертатися в дата центр, через професійний програмний інтерфейс.

Безпека зберігання та стабільність доступу до відеоархіву забезпечується вищим ступенем надійності професійних центрів обробки даних, що недосяжно для локальних сховищ.Доступ до відеоархіву надається у вигляді професійного програмного інтерфейсу для роботи з відеоархівом.

Найлегший і надійний спосіб налаштувати онлайн трансляцію з камер на сайті.

До недоліків слід віднести обмежену доступність апаратного забезпечення - трансляція відео з камери на хостинг можливо тільки з прошивкою вендора, або з використанням комп'ютера, а також постійні витрати на абонентську плату.

Великі світові виробники камер відеоспостереження надають послуги хостингу відео. GeoVision зі своїм хмарним сервісом MyGvCloud. Сервіс надає кілька цікавих і поки ще що не так часто присутніх можливостей - стрім з IP камери безпосередньо в YouTube. Додатки для відеоспостереження на Android TV та Apple TV.

4) Доступ до онлайн перегляду і відеоархіву на NVR або NAS і бекап відеоархіву в хмару.

Ключова відмінність від попереднього пункту в тому, що якщо ви захочете переглянути відеоархів, програмний клієнт буде звертатися до локального сховища на NVR або NAS, і тільки в тому випадку якщо локальний відеоархів втрачений ви будете звертатися в хмару.

Безпека зберігання відеоархіву забезпечується вищим ступенем надійності центру обробки даних. Практично необмежений вибір IP камер.

До недоліків слід віднести високу вартість зберігання відео, низьку пропускну здатність каналів зв'язку, постійні витрати на абонентську плату. На відміну від попереднього пункту, доступ до перегляду відеоархіву на хостингу надається у вигляді доступу до файлів, що ускладнює роботу з ним.

При розгляді завдань щодо створення резервної копії, неодмінно постає питання куди зберігати бекап. Розглянемо коротко питання інтеграції з сервісами зберігання даних:

– безкоштовні сервіси зберігання файлів як правило обмежують розмір одного завантаження;

− мережеві сховища можуть бути з обмеженим максимальним розміром збережених даних і безрозмірні, наприклад Amazon S3, плата стягується за обсяг реально, що зберігається;

− устаткування підтримує копіювання на хмарні сервіси зберігання.

Копіювання може працювати в декількох режимах:

− просте завантаження - в цьому випадку старі дані потрібно видаляти вручну, особливо це важливо для сервісів, що обмежують максимальний розмір сховища;

− синхронізація - пристроїв зберігання відеоархіву працює в режимі циклічної перезапису, сервіс зберігання синхронізує весь обсяг;

− бекап - створення резервної копії даних на певний момент часу, можна створювати і зберігати практично необмежену кількість бекапів.

Розглянемо найпопулярніші сервіси та обладнання, як приклад, оскільки список набагато більший.

Google Drive, сервіс Qlync дозволяють зберігати відео з сумісних IP камер безпосередньо в Google Drive, список сумісних камер не великий, але в ньому є наприклад камери Zavio непогано представлені на українському ринку.

Dropbox - мережеві відеореєстратори (NVR) Tantos дозволяють відправляти відео в хмару, наприклад - TSr-NV32251, TSr-NV16241, TSr-NV08241

Amazon S3 - мережеві сховища для відеоспостереження від Synology .

Насправді резервне копіювання можна налаштувати практично в будь-який сервіс зберігання, вибір обладнання великий, в тому числі і досить екзотичний - Microsoft OneDrive, Google Cloud Storage ElephantDrive, Amazon Glacier, Microsoft Azure, HiDrive, hubiC, Backblaze B2, Baidu Cloud , Box, Amazon Drive тощо.

Тепер коли можливості хмарного відеоспостереження розподілені по чотирьом категоріях варто розглянути про переваги хмарного відеоспостереження і його проблеми.

2.2 Побудова логічної структури системи відеоспостереження

Можливості хмарного відеоспостереження не обмежуються тільки віддаленим переглядом онлайну і відеоархіву, але дозволяють не тільки бачити, а й чути, і навіть спілкуватися голосом в прямому ефірі [10,11]. Можна підключити всіх до відеосервера одночасно, переглядайти зображення онлайн з різних серверів на одному клієнтському місці.

Для запропонованої логічної структури хмарного відеоспостереження потрібно встановити наступні вимоги:

– PlugNPlay - більшість виробників, прагнуть зробити своє обладнання доступним для підключення та налаштування навіть недосвідченими користувачами. У більшості випадків достатньо просто відсканувати QR код додатком встановленим на мобільний телефон, і можна відразу насолоджуватися переглядом;

– мультиплатформеність - Android, iPhone OS, Windows Phone, Android TV, Apple TV, Mac OS, Windows, Linux - більшість вендорів розробляють додатки як мінімум на найбільш популярних платформах. Сюди можна додати і кросбраузерність;

– повідомлення - спливаючі в додатках push-повідомлення, СМС і E-mail повідомлення не тільки не дозволить вам пропустити критично важливу подію, але і позбавляє вас від необхідності постійного моніторингу. Вже сьогодні ми маємо не маленький список подій, настання яких потрібно відстежувати. Детекція руху у виділеній області, детекція звуку мікрофоном,

детекція перетину лінії, входу/виходу з області, залишених або зниклих предметів. Також ви можете отримувати повідомлення про відключення камер або носіїв відеоархіву, про розрив мережі, конфлікт IP-адрес;

– права доступу - розмежування прав доступу, стандартний функціонал програмного забезпечення для відеоспостереження. Для хмарного відеоспостереження він знайшов новий сенс, ви можете надати доступ всім співробітникам до певної групи камер, або всім відвідувачам вашого сайту, або тільки клієнтам, або тільки перегляд, аботількио доступ до архіву. Наприклад, чому б не дати доступ усім мешканцям до системи відеоспостереження житлового багатоквартирного будинку;

– інтеграція - уже зараз додатки для відеоспостереження дозволяють відслідковувати охоронні датчики, датчики температури і вологості.

Основний фактором, що стримує розвиток хмарного відеоспостереження є канали зв'язку. За даними World Wide Web Foundation в світі середня швидкість вихідного каналу становить 5 Мбіт / с, що входить 15 Мбіт/с [10,11]. Щоб записати відео з однієї камери в HD орматі (1280 * 720) з частотою 25 кадрів в секунду, з використанням H.264 кодека, з середньою інтенсивністю руху вам потрібно мати канал приблизно рівний 3,2 Мбіт/с. На об'єкті, що досліджується, канал передачі рівний 10 Мбіт/с. Тому потрібно використовувати смарт кодеки H.264 + від HikVision і Zipstream від Axis, вони вже зараз вони дозволяють зменшити бітрейт до 70%.

На даний час H.265 кодек, підтримує багато обладнання. Експерти вважають, що час коли він стане новим стандартом в відеоспостереження вже не за горами.

Також є можливість використовувати відеокамери з вбудованою відеоаналітикою, вони дозволяють обробляти не декодований потік на самій камері, і відправляти по мережі вже результати обробки.

Оцифрована інформація компресується до 1000 разів, траспортується з використанням комп'ютерних мереж на будь-яку дистанцію, аналізується

комплексними програмними і апаратними процедурами з метою ідентифікації переміщення в кадрі, наявність цифрового збільшення для потрібного зображення, зберігання оцифрованих даних дозволяє здійснювати цифрова камера у порівнянні ніж аналогова.

Для оцифровки відеоінормації використовують пристрої - фреймграббери. Залежно від мети виробника при формуванні граббера можуть бути застосовані багато технологій, оскільки існує велика кількість схем, якими вона може доокомлектовуватися. Контролери оцифровки бувають двох видів: застосовуються для промислових і наукових застосувань або для роботи в сфері мультимедіа. Граббери, що застосовуються в наукових цілях для контролю процесу виробництва, конвертують відеоінформацію з досить високою точністю, вносячи мінімальні спотворення. Мультимедійні контролери на початку конвертують інформацію, а потім з естетичною метою перетворюють його так, щоб зображення було більш чіткішим. Через абсолютно різні сфери використання контролери двох різних видів не можуть бути взаємозамінними, хоча деякі виробники мультимедійних плат надають їх як "універсальне" вирішення для всіх тидів застосувань.

Мультимедійний контролер укомплектовується таким набором мікросхем, які значно перетворюють відеоінформацію, тим самим приносячи більшу кількість шуму і артефактів. Ці зміни, які не наявні в первісному сигналі, можуть принести помилки вимірювання на наступних етапах обробки і аналізу даних. При застосуванні даних контролерів в застосуваннях, які потребують високої точності (інспектування цілісності поверхонь, технологічні вимірювання, мікроскопія), внесені зміни можуть довести до помилкових результатів.

Контролери оцифровки (грабери) відеозображення дозволяють проводити захоплення і аналіз інформації, що несе візуальні дані. Як правило, вони являють собою плати, що приєднуються до однієї з

комп'ютерних схем. Плата трасформує відеовихідне зображення джерела відеосигналу в потік даних, які можуть зберігатися в цифровому вигляді, а також аналізуватися, оброблятися і відображатися на екрані дисплея. Відеоінформація може приходити від дуже різних джерел: спецвідеомагнітофона, відеокамери, мультиплексора з підключеними до нього камерами телевізійного тюнера і схожих за функціоналом пристроїв. Ці джерела можуть надавати композитний (цілісний) відеосигнал, а також сигнали синхронізації або компонентний відеосигнал, коли різні складові сигналу траспортуються по окремих лініях. Крім того, кольорові відеосигнали можуть містити одну з прийнятих в світі класичних підходів кодування кольору, - NTSC, PAL, SECAM, або їх різновиди [12-15].

Оцифроване зображення, одержане в результаті відеограбінгу, отримує додатково наступні характеристики:

- роздільну здатність, яка встановлює величину компонентів зображення і використовує кількісь точок (пікселів) по горизонталі і вертикалі (256x256, 640x480, 768x576 і ін.);

- відношення ширини пікселя до його висоти (зазвичай це 1: 1, але бувають і інші, наприклад, 4: 3);

- глибина формування кольору - ідентифікує кількість кольорів або відтінків одного кольору, визначається в бітах (8 біт - 256 кольорів (відтінків сірого для монохромного зображення). 10 біт - 1024, 16 біт - 65 536);

- частота кадрів (Frames Per Second - FPS), швидкодія, з якою кадри замінюють один одного за одиницю часу, класично за секунду 25 кадрів в секунду хватає для того, щоб зображення було послідовним, без шумів.

Контролери оцифровки відеозображення можуть бути різних видів, вони відмінні за формою і розмірами, але не дивлячись на різницю в характеристиках і дизайні, вони, за невеликими винятками мають спільні принципи роботи.

Приймання відеосигналу - це компонент, на який надхадить сигнал з приєднаного пристрою. Багато контролерів відеооцифрування мають вмонтований мультиплексор - електронний перемикач, який надає можливість обирати один з декількох видеовходів. Отже, до окремих плат можна приєднати до чотирьох (найбільш доцільно) і більше джерел відеосигналу. До того ж, для забезпечення деяких цілей багатомонохромні грабери мають так званий "колірний ефект" або фільтри кольоровості. Необхідність одержання монохромного зображення від кольорового джерела обґрунтовується тим, що кольоровий елемент сигналу може бути основою для інтерференційних картинок, які зменшують якість зображення. Фільтри кольоровості усувають колірний елемент для більш якісного приймання сигналу і більш точного його аналізу.

Деякі контролери надають можливість програмного налаштування характеристик діапазону прийому сигналу (зміна заданих за замовчуванням параметрів), це дозволяє одержати краще за якістю зображення при обробці сигналу мінімальної потужності. Можливість такого налаштування порту прийому точно під параметри вхідного сигналу надає можливість домогтися точної оцифрування.

Синхронізація - цей блок формується з систем хронометражу, синхронізації і управління прийомом відеозображення. Разом з блоком конверсії вони формують "серце" контролера оцифровки. Схема хронометражу може функціонувати як на фіксованій частоті (в разі контролерів, які отримують відеосигнали стандартних форматів), так і на частотах, що задаються програмно (в разі використання контролерів, які отримують нестандартні відеосигнали чи сигнали малопоширених кодувань). Робота схеми хронометражу жорстко комбінується з роботою схеми синхронізації, яка синхронізує такти схеми хронометражу і імпульси вхідного відеосигналу.

Плати оцифровки можуть мати розширену схему синхронізації на випадок відеосигналів, що містять мале співвідношення сигнал/шум або не формують зафіксовану, змінну згодом, частоту. Ці схеми відновлюють пошкоджену/змінену частотність імпульсів шляхом укомплектування пропущених імпульсів і ігноруючи інші. Такі схеми зазвичай необхідні для отримання чіткого зображення від дуже "шумливих" джерел відеосигналу, таких як відеомагнітофони або відеокамери, що траспортують сигнал по дуже довгому кабелю.

Схема керування прийомом зображення надає можливість зовнішнім сигналам вмикати і підготовити плату для захоплення вхідного сигналу. Подібні сигнали часто пов'язані з будь-якими процесами, такими, як переміщення об'єктів зйомки по конвеєру, або іншими промисловими ситуаціями. Ця схема потрібна там, де необхідна тільки періодична робота плати, а не постійна.

Блок обробки відеозображення встановлює інформацію після того, як зображення було оброблено АЦ конвертером. Таблиці перекодування (Look-UpTables - LUTs) застосовуються для обробки інформації про зображення і зазвичай бувають двох випів: вхідні (Input LUTs - ILUTs) і колірні (Palette-matching LUTs). Вхідні таблиці перекодування застосовуються для зміни цифрових даних зображення в реальному часі, а також для інверсії і зміни значень шкали півтонів (шкали відтінків сірого кольору). Зазвичай, після того, як зображення буде транспортовано в комп'ютер, всі ці дії можна сформувати, застосовуючи програмне забезпечення, але за допомогою апаратних пристроїв плати це буде сформовано набагато скоріше. Кольорові таблиці перекодування, які досить часто наявні в монохромних контролерах оцифровки, застосовуються для керування палітрою кольорів комп'ютера для того, щоб завантажені програми не отримували монохромні картинки з колірними аберацієями.

Схема масштабування і виділення надає можливість зменшити цифрове зображення (а в деяких випадках - збільшити) як по осі X так і по осі Y перед тим, як передати його на комп'ютер. Виділення надає можливість обрати цікаву ділянку зображення і не враховувати всю інформацію, що залишилися. Керування розміром і виділення потрібного елемента зображення зменшує час обробки і транспортування даних. Це потрібнол для застосувань, які критичні до часу, коли необхідно обробити багато об'єктів, наприклад, зображення обличчя людей на прохідній, номерів машин на активному автошляху.

Якщо блоки прийому і конверсії сформовані з помилками, то вони несуть шуми, що сильно змінюють відеодані. Головним є не властивості внесеного платою шуму: сумарна нелінійність і середньоквадратичне відхилення, які обчислюються в одиницях, що називаються lsb (Least Significant Bit - молодший значущий розряд). Lsb характеризує точність цифрового представленя сірих тонів. Сумарна нелінійність оцінює відхилення сірого кольору, одержаного контролером, від сірого кольору вихідного зображення, а середньоквадратичне відхилення - перешкоди, що надходять від схем плати. Чим менші значення обох параметрів, тим вища якість функціонування контролера. Якщо вони не перевищують 0,5 lsb, то це формує, що даний граббер є хорошим інструментом для оцифровки зображення.

У різних тидів кодувань сигналу співвідношення довжини пікселя до його висоти може бути різним. Так, в форматі RS-170 сторони співвідносяться, як 4:3. Відношення сторін пікселя тісно пов'язане з процесом обробки зображення. У багатьох контролерів оцифровки, що працюють з частотою 60 Гц, це співвідношення дорівнює 5:4, тоді як у більшості грабберів, що функціонують з частотою 50 Гц, воно рівне 3:2. Інші плати захоплення відеозображення надають можливість ормувати відношення сторін пікселя програмним чином. У тому випадку, коли

картинка траспортується і відображається з однаковим співвідношенням сторін пікселя, це не віграє великої ролі, форма об'єктів не змінюється, квадрати залишаються квадратами, а окружності - колами. Співвідношення сторін пікселя варто взяти до уваги при роботі деяких спеціальних операцій, таких як формування площі ділянки зображення шляхом підрахунку компонентів, його складових, або вигин обраної області зображення. Крім того, відношення довжини і висоти пікселя є дуже важливим, якщо результуюче зображення повинно задовольняти графічним стандартам, тому, якщо застосування вимагає точного "попіксельного" обчислення, потрібно переконатися, що графічні компоненти зображення є квадратними (мають співвідношення сторін 1: 1).

При запису зображення зазвичай застосовуються по 8 біт (1 байт) для подання 256 рівнів яскравості червоного, зеленого і синього кольорів (RGB). Отже, для запису одного компонента зображення (пікселя) потрібно 3 байта пам'яті. Стандартний відеокадр формату 352x288 пікселів потребує 304128 байтів, а зображення на екрані дисплея навіть при роздільній здатності 640x480 формує майже цілий мегабайт.

Застосування класичних алгоритмів компресії "без втрат", таких як RLE (кодування довжин серій) або LZW (метод Зива-ЛемпелаУелча), не знаходить вирішення проблеми, оскільки критичні для них коефіцієнти компресії (2-3 в разі чорно-білих напівтонових або 1,5-2 для RGB зображень) завершено недостатні для більшості застосувань. Коефіцієнт компресії, що досягається при застосування будь-якого способу, залежить від параметрів зображення. Наприклад, одноколірний фон в будь-якому випадку компресується краще ніж наявністю великої кількості дрібних деталей зображення.

Повнокольорові 24-бітові зображення можна компресувати шляхом синтезу зображення зі штучною палітрою і використанням кодування довжин серій в поєднанні зі статистичними кодуванням, але при цьому

максимальний коефіцієнт компресії буде не більше 3-5 щодо вихідного зображення, причому головна компресія здійснюється за рахунок переходу від RGB до 256-кольоровому зображенню зі штучною палітрою, причому зміни, що формуються при такому переході, незворотні, і вже ця обставина не дозволяє застосовувати такий спосіб компресії достатнім.

Більшість класичних методів компресії як нерухомих, так і відеозображень, що формують компресію в десятки, а іноді в сотні разів, надають деякі втрати, тобто відтворене зображення не збігається в точності з вихідним. Втрати ці пов'язані з відмовою від транспортування або деякого "загрубіння" тих елементів зображення, чутливість до точності відтворення яких у людського ока мінімальна.

2.3 Розробка політики захисту корпоративного хмарного відеоспостереження

Серед основних загроз, що виникають при впровадженні систем мережевого відеоспостереження потрібно виділити наступні.

1) Механічні силові дії.

Удар, взлом, розтин, вигин, розрив, і т.п., що викликають повне руйнування або пошкодження компонентів комплексу, порушення електричних зв'язків або зміну орієнтації камер. Ймовірні об'єкти впливу: лінійна частина системи (кабелі, підсилювачі, кронштейни, корпуси і термо-кожухи, поворотні пристрої, апаратура телеметрії і інші компоненти, вилучені від постів охорони). Методи захисту: фізичний захист компонентів (використання ударопрочних конструкцій корпусів, кронштейнів, і т.п .; прихований монтаж і прокладка кабелів в сталевих трубах).

Обмеження доступу до компонентів (установка компонентів в важкодоступних місцях, захист компонентів або підступів до них за допомогою засобів охоронної сигналізації).

Контроль стану компонентів (перевірка правильності функціонування камер, періодичний зовнішній огляд компонентів з перевіркою заданих установок).

2) Електромагнітні впливи.

Відключення мережі змінного струму, створення електро- або радіоперешкод. Ймовірний об'єкт впливу:всі компоненти системи.

Методи захисту: організація електроживлення (енергопостачання по першій категорії, використання джерел безперебійного і резервного живлення з автоматичним перемиканням).

Підвищення перешкодозахищеності (правильний вибір сигнальних кабелів і кабелів живлення, використання ізолюючих трансформаторів і мережевих фільтрів, рознесена прокладка кабелів живлення і сигнальних кабелів; прокладка кабелів найкоротшим шляхом, екранування і заземлення).

3) Керуючі впливи на апаратну частину системи за допомогою спеціальних пристроїв.

Зміна установок регульованих параметрів (фокусна відстань, орієнтація камер, і т.п.), неузгодженість ліній зв'язку, блокування реального сигналу або впровадження помилкових даних. Об'єкти впливу: лінійна частина системи (камери, апаратура телеметрії, лінії зв'язку, їх ланцюга і ділянки, найбільш схильні до зовнішніх впливів). Методи захисту: підвищення перешкодозахищеності (правильний вибір сигнальних кабелів; прокладка кабелів найкоротшим шляхом, екранування і заземлення-ня).

Обмеження доступу до компонентів (установка компонентів в важкодоступних місцях, прихований монтаж і прокладка кабелів в сталевих трубах; захист компонентів або підступів до них за допомогою засобів охоронної сигналізації).

Контроль стану компонентів і зони сприйнятливості системи (перевірка правильності функціонування камер, періодичний зовнішній огляд компонентів з перевіркою заданих установок, пошук сторонніх сигналів управління в зоні сприйнятливості системи за допомогою спеціальної апаратури).

4) Вплив на програмне забезпечення.

Зміна алгоритму роботи, внесення вірусів, знищення програми. Об'єкти впливу: інтелектуальна частина системи (програмовані мультиплексори, матричні комутатори, відеоменеджер, системні блоки комп'ютерів, і т.п.).

Методи захисту: обмеження доступу до програмного забезпечення (установка компонентів в спеціальних сейфах на центральному посту охорони або в кабінеті керівника об'єкта, захист компонентів або підступів до них за допомогою засобів охоронної сигналізації, використання паролів і кодів доступу).

Контроль стану системи (використання коригувальних тест-програм, періодична перевірка відповідності алгоритму роботи системи заданому).

5) Вплив на відеоархіви.

Зняття копій, підміна, розкрадання або знищення відеоінформації.

Ймовірний об'єкт впливу: засоби запису, відтворення і зберігання інформації (відеомагнітофони, відеопринтери, жорсткі, гнучкі, оптичні та компакт-диски, відеокасети, лістинги, доступ до хмарних технологій збереження інформації і т.п.).

Методи захисту: обмеження доступу до компонентів (установка компонентів і зберігання архівних матеріалів в спеціальних сейфах на центральному посту охорони або в кабінеті керівника об'єкта, використання паролів і кодів доступу до архівних матеріалів; захист компонентів, архівних матеріалів або підступів до них за допомогою засобів охоронної сигналізації).

Контроль стану компонентів і архівів (перевірка працездатності компонентів, періодичний перегляд і аналіз архівних матеріалів, знищення зайвої інформації).

Організація резерву (резервування компонентів; створення архівів-копій з зберіганням їх в іншому недоступному місці).

Якщо аналізувати хмарні відео сервіси зберігання даних, вони досить часто стають лідируючим каналом витоку інформації. За останні роки 50% витоку інформації відбулося через хмарні сервіси. Мова звичайно йде про все різноманіття хмарних сервісів, нас же в першу чергу цікавлять як мінімум сервіси пов'язані з відеоспостереженням, як максимум кібербезпека систем відеоспостереження в цілому.

Аналізуючи події останніх років, можна визначити, що ситуація в відеоспостереження навряд чи відрізняється в кращу сторону.

Ботнет Mirai, частиною якого були IP камери, призвів до перебоїв значної частини глобальної мережі інтернет

Критичну вразливість виявили в глобальних хмарних серверах HikVision. Вразливості в системі безпеки камер виявляються навіть у таких грандів як Axis [16].

Незважаючи на це маркетологи будь-якого хмарного сервісу заявляють безпеку в список своїх переваг, правда їх же юристи в призначених для користувача угоди, які ніхто не читає, з ними категорично не згодні.

Компанія не може і не гарантує, що використання програмного забезпечення, веб-сайту, послуг або продуктів абсолютно безпечно.

Ось так, написано в призначених для користувача угоди всіх компаній пропонують послуги хмарного відеоспостереження.

Це ні в якому разі не привід відмовлятися від VSaaS.

Тим більше що експерти заявляють, що до 2020 року, буде усвідомлено проблеми кібербезпеки. А як відомо усвідомити проблему це на 50% її вирішити.

Одним із шляхів вирішення безпеки хмарного сервісу є використання HTTPS.

IP-камера здатна перед відправкою по мережі шифрувати відеосигнал, що запобігає можливості його несанкціонованого перегляду або його підміни. Систему можна також налаштувати на аутентифікацію з'єднання за допомогою зашифрованих сертифікатів, які сприймаються конкретною мережевою камерою, усуваючи таким чином ймовірність, що хтось уклиниться в лінію.

Шифрування відеоархіву на даний момент досить широко використовуються в відеоспостереження. Ezviz наприклад шифрує відео, яке записує на SD карті, тобто просто вийнявши карту доступ до відеоархіву зловмисник не отримає.

A Synology дозволять не тільки резервувати дані в режимі реального часу, зводячи до мінімуму ризики при непередбачених ситуаціях, а й шифрувати за допомогою алгоритму AES-256 дані перед завантаженням в хмару[17-19].

Сучасні реалії такі, що вразливості знаходять і в IP камерах будь-яких вендорів, і на перший план виходить не стільки сам факт вразливості, а те як компанії швидко їх закривають, випускаючи оновлені прошивки. Тому особливо важливим стає вже ваша реакція і оновлення прошивки саме на вашій камері. А оновлення прошивок це - доступ до камери, логіни і паролі, а якщо камер десятки, а якщо сотні. Та й процес відстеження виходу нових версій прошивок теж та ще задача. А все разом це титанічна праця. Вибираючи вендора потрібно звернути увагу на те як організована робота з відстеження нових прошивок, та їх оновлення.

Наприклад, програмне забезпечення для моніторингу IDIS Center вміє відслідковувати вихід нових прошивок, та автоматично оновлювати прошивки (запуск процесу вручну, саме оновлення відбуваються

автоматично), в тому числі і на віддалених камерах. Природньо тільки на камерах власного виробництва.

3 ТЕХНІЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1 Технічна реалізація системи відеостереження

Для організації системи відеоспостереження в організації потрібно [20]:

- визначити кількість камер та їх розташування;
- вибрати моделі камер для кабінетів, залів і фасадів будівлі;
- вибрати відеореєстратор виходячи з кількості і характеристик камер;
- вибрати блоки живлення або POE-комутатори.

Оскільки для організації відеоспостереження продуктового магазину потрібно використовувати тільки внутрішні камери доцільно використати камери 24 серії компанії Hikvision - відмінний варіант ширококутних камер для кабінетів та залів магазину, зокрема Hikvision DS-2CD2420F-I.

Проста IP-камера Hikvision легко монтується у стелю або на стіну. Модель забезпечує якісну картинку, широкий динамічний діапазон і компенсацію заднього засвічення. Оснащена яскравим ІЧ-діодом, датчиком руху PIR, і вбудованим мікрофоном з динаміком. Є можливість робити запис на MicroSD-карту. Доступні додатки для смартфона.

Зовнішній вигляд камери представлено на рисунку 3.1. Технічні характеристики камери подані у Додатку А.

Враховуючи специфіку приміщення та функціональні задачі корпоративного відеоспостереження продуктового магазину доцільно використати 7 камер: 4 камери по кутах торгового залу, дві камери над простором касирів та одну в кабінеті директора.

Оскільки дана серія камер не підтримує POE потрібно буде забезпечити подачу живлення через виту пару до камер, а сам блок живлення розмістити поряд з реєстратором у серверній магазину.

Рисунок 3.1 – Камера Hikvision DS-2CD2420F-I

Для забезпечення формування локального відеоархіву необхідно вибрати відеореєстратор виходячи з кількості і характеристик камер. Звичайно, можна записувати відео на комп'ютер. І якщо в організації одна - три камери, це має певний сенс. Але досвід показує, що навіть за невеликої кількості камер, краще використовувати відеореєстратор.

Hikvision DS-7616NI-E2 - відеореєстратор з великою пропускною здатністю, що досягає 100 Мбіт/с. До нього можна під’єднати до 16 камер різних виробників. З метою забезпечити мінімальні затрати при потребі збільшити кількість та якість камер доцільно використати саме відеореєстратор на 16 камер, що дасть в майбутньому можливість розширення площі відеоспостереження.

Роздільна здатність відеозображення, що дозволяє переглядати відеореєстратор, через підключені камери досягає 5 Мп. Продуктивність реєстратора Hikvision DS-7616NI-E2 достатньо висока й дає оператору можливість спостерігати відео онлайн або відтворювати його у роздільній здатності: 5 MP, 3 MP, 1080 P, 720 P, VGA, 4 CIF та ін. Зовнішній вигляд

відеореєстратора представлено на рисунку 3.2 Завдяки аудіовходам і виходами, а також способом запису звуку з IP-камер користувач може записувати і прослуховувати звук з камер.

Рисунок 3.2 – Зовнішній вигляд реєстратора Hikvision DS-7616NI-E2

У відеореєстратора Hikvision DS-7616NI-E2 є можливість формувати відеоархіви, тому його можна додатково укомплектовувати двома жорсткими дисками з об'ємом кожного не більше 4 Тб. Для швидкого копіювання забезпечено швидкісний USB 3.0 порт. Детальні технічні характеристики реєстратора подано у додатку Б.

Управління реєстратором можна здійснювати через локальну мережу, або через віддалений доступ за допомогою персонального комп'ютера чи інших мобільних пристроїв.

Можна використовувати один з двох типів живлення: блоки живлення або PoE. Блоки живлення в комплекті не йдуть. Тому, використано один блок живлення і через використаня не задіяних пар Ethernet забезпечено живлення відеокамер.

Для забезпечення доступу до інтернет локальної мережі магазину і відеореєстратора через провайдера Ternet використано TP-Link 300 Мбит/с безпроводовий маршрутизатор серии NTL-WR840N.

На рисунку 3.3 представлено зовнішній вигляд маршрутизатора.

Основні технічні характеристики пристрою представлено у додатку В.

Рисунок 3.3 – Зовнішній вигляд маршрутизатора NTL-WR840N

Доцільно розглянути основні характеристики даного пристрою. Швидкість бездротової передачі даних до 300 Мбіт / с - ідеальний варіант для базових і ресурсоємних завдань. Швидка настройка захисту бездротової мережі одним натисканням кнопки WPS. Контроль пропускної здатності по IP-адресі дозволяє адміністратору призначати допустиму ширину каналу для кожного комп'ютера чи пристрою.

Бездротовий міст WDS дозволяє збільшити зону стабільного покриття бездротової мережі. Підтримка IGMP Proxy, режиму "міст" і 802.1Q TAG VLAN для послуги IPTV без затримок.

Маршрутизатор TL-WR840N являє собою комбінований пристрій для проводового/бездротового доступу, призначений спеціально для використання в малих організаціях. Маршрутизатор TL-WR840N забезпечує виняткові показники бездротової передачі даних, роблячи його ідеальним для потокового перегляду відео у форматі HD, а також для VoIP і онлайн-ігор. Кнопка WPS (Wi-Fi Protected Setup) забезпечує шифрування WPA2, яке дозволяє захистити мережу від зовнішніх загроз.

TL-WR840N - це високошвидкісний пристрій, що підтримує стандарти зв'язку IEEE 802.11b/g/n. Завдяки підтримці 802.11n пристрій дозволяє встановлювати бездротове з'єднання на швидкості до 300 Мбіт/с, що відповідає вимогам більшості невеликих мереж.

Технологія CCA (оцінка доступності каналу) дозволяє уникати конфліктування каналів при передачі даних. Завдяки функції вибору і об'єднання каналів продуктивність бездротового з'єднання істотно зростає.

Контроль пропускної здатності за IP-адресою дозволяє адміністраторам визначати обсяг пропускної здатності, що виділяється кожному комп'ютеру в мережі. До пристрою додається компакт-диск з майстром швидкого налаштування, який дозволяєть крок за кроком налаштувати свій пристрій і мережу, а також забезпечити її захист.

3.2 Встановлення та налагодження системи відеоспостереження

Для забезпечення доступу до пристроїв відеоспостереження (реєстратора чи камер) потрібно здійснити процедуру переадресації портів на маршрутизаторі.

Переадресація портів - це створення шляху, по якому ми можемо віддалено зайти на пристрій в нашій локальній корпоративній мережі[21]. В наному випадку, на відеореєстратор, щоб переглянути на підключені до нього камери в реальному часі, подивитися запис в архіві або змінити будь-які налаштування.

Якщо переадресація портів не встановлена, то максимум, куди ми можемо потрапити з Інтернет - ця на наш роутер (по-іншому - маршрутизатор). Це та перешкода, рубіж, за яким починається світ локальної мережі - пристроїв в нашому магазині, які підключені до Інтернету.

Як правило, меню, в якому знаходиться потрібна нам функція, називається Віртуальні сервери. Зайшовши в нього, діємо аналогічно розглянутим нижче прикладами.

Відкриваємо свій браузер і вписуємо в адресний рядок локальну адресу нашого роутера. За замовчуванням у TP-LINK він такий: 192.168.0.1.

Ім'я користувача: admin.

Пароль: admin.

Після введення пароля відкривається інтерфейс роутера в зелених тонах. У лівом вертикальному меню і знаходимо там пункт Переадресація (Forwarding). Розкривши цей пункт, тобто, просто клікнувши по ньому, заходимо на підпункт Віртуальні сервери (Virtual Servers) (рисунок 3.4).

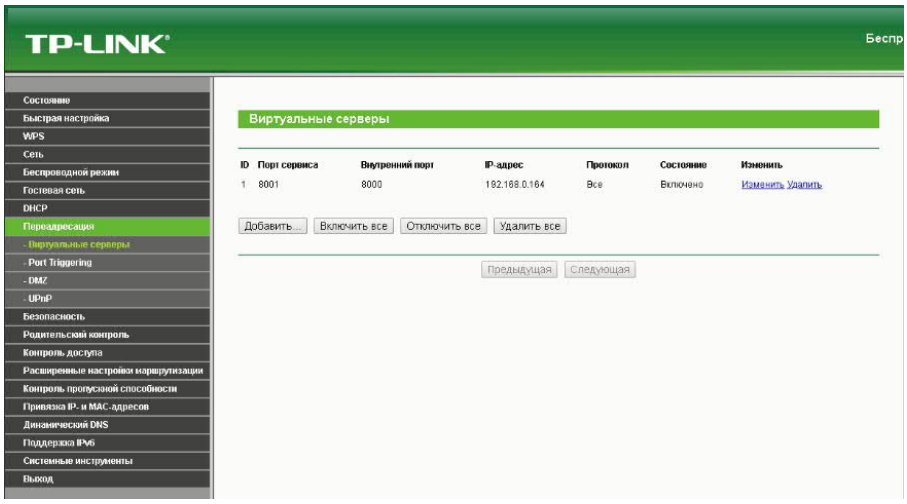

Рисунок 3.4 – Налаштування маршрутизатора локальної мережі

На сторінці, шукаємо єдину активну кнопку Додати (Add New) і натискаємо її.

Тепер нам треба заповнити поля, щоб ззовні можна було потрапити на відеореєстратор.

Порт сервісу (Service Port) ставимо будь-який, який нам більше подобатися, наприклад 8001, як на рисунку 3.5.

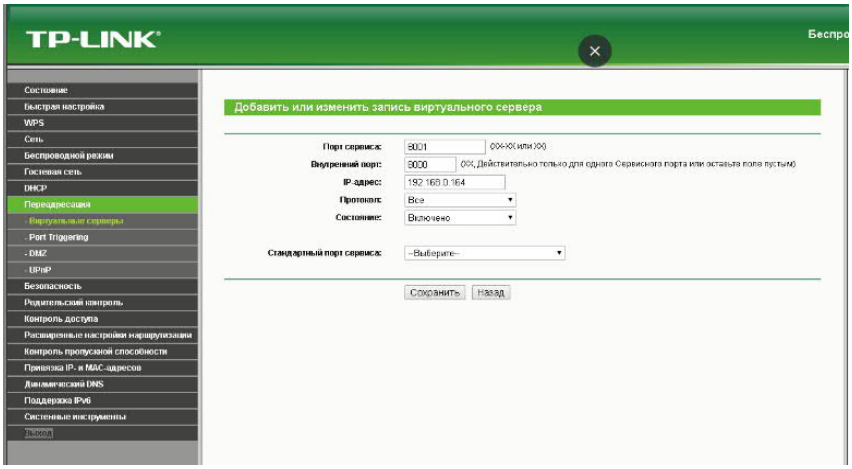

Рисунок 3.5 – Перенапрвлення портів на маршрутизаторі

Цей порт вказуємо при вході на наш пристрій з мережі інтернет в спеціальній програмі або в адресному рядку браузера через двокрапку після основної адреси.

Внутрішній порт (Internal Port), навпаки, жорстко лімітований. Він зазначений в реєстраторі або IP камері і за замовчуванням, як правило, 8000.

IP адреса (IP Address) - це внутрішня локальна адреса нашого відеореєстратора. Його можна або подивитися в самому реєстраторі, або використовуючи спеціальну програму, яка бачить всі пристрої в мережі.

Тепер нам треба заповнити поля, щоб ззовні можна було потрапити на відеореєстратор.

В даному випадку показаний приклад перенаправлення порту 8000, який використовується для віддаленого відеоспостереження на мобільних додатках.

Тепер для того, щоб потрапити на реєстратор з інтернету, досить вказати в програмі або адресному рядку зовнішню IP адресу вашої мережі і додати порт, щоб роутер ввічливо провів вас в пункт призначення.

Сучасні тенденції не оминули стороною системи відеоспостереження. Компанія Hikvision запустила власний хмарний сервіс EZVIZ Cloud - гра слів Easy і Vision [22 -24]. Він призначений для широкого кола використання, а це значить, що отримати доступ до хмари може будь-яка людина.

Завдяки хмарному сервісу EZVIZ, який працює на основі моделі SaaS, користувач може отримувати відео з будь-якої точки світу за допомогою IP-камери Hikvision. Ви можете спостерігати за працівниками в магазині, новою нянею своєї дитини, літніми батьками, будинком, складом та іншими об'єктами, що вимагають постійного спостереження. Якщо у камери є мікрофон, ви зможете підтримувати двосторонній аудіозв'язок. EZVIZ дозволяє робити фотографії, переглядати архів відеозаписів, отримувати тривожні push-повідомлення, залишати повідомлення в камері й навіть дізнаватися температуру і вологість у приміщенні, за яким ведеться відеоспостереження.

Ще одна перевага хмари в тому, що для її використання підходить як статична, так і динамічна IP-адреса.

Хмара EZVIZ - це глобальна платформа для зберігання відеозаписів, яка зв'язується з смарт-пристроями і забезпечує шифрування банківського рівня для користувачів.

Інформаційна безпека забезпечується відповідно до сертифіката ISO / IEC 27001. Перед збереженням на хмарних серверах дані піддаються подвійному шифрування. Відеопотоки шифруються на всіх стадіях (E2EE).

В хмарі EZVIZ алгоритми штучного інтелекту (ШІ) використовуються від центру до кінцевих мереж і пристроїв. Це дозволяє знизити навантаження на хмару шляхом перенаправлення даних на обробку кінцевим мережам і пристроям, які підтримують алгоритм ШІ і технологію поглибленого навчання.

Користуватись хмарним сервісом Hikvision безпечно, не потрібно хвилюватися про несанкціоноване проникнення - компанія гарантує достатній рівень безпеки EZVIZ.

Для того, щоб почати користуватися хмарою, потрібно виконати всього кілька дій. Потрібно зайти на сайт хмари EZVIZ і натиснут кнопку "Register". Заповнити усі необхідні для реєстрації поля (рисунок 3.6).

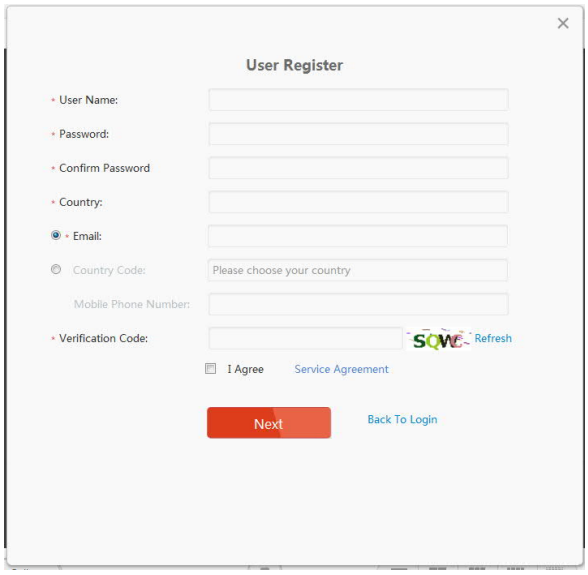

Рисунок 3.6 – Реєстрація в хмарному сервісі EZVIZ

Після того, як було здійснено реєстрацію і пройдено підтвердження реєстрації, потрібно зайти у свій особистий кабінет. Було запрпоновано завантажити та встановити додаткове програмне забезпечення EZVIZ studio.

Для підєднання камери чи відеореєстратора до хмарного сервісу ком'ютер повинен бути в одній локальній мережі з ними, а також потрібно знати унікальний код камери, який вказаний на наклейці на самій камері.

Тепер знову потрібно зайти в особистий кабінет на сайті й натиснути кнопку "Add Now", сервіс почне пошук вашої камери. Якщо EZVIZ її виявить, натискайте на ім'я камери й сервіс запитає верифікаційний код (код підтвердження), розташований на камері. Якщо камера не розпізналася, потрібно додайти її вручну за серійним номером (рисунок 3.7).

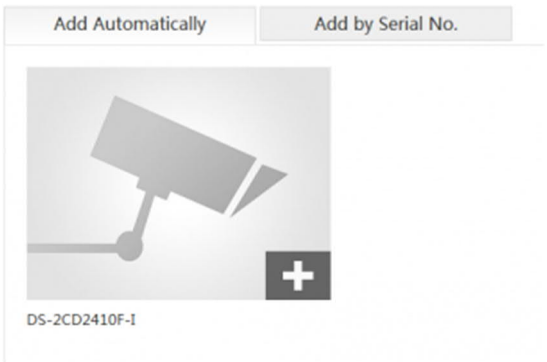

Рисунок 3.7 – Додавання пристроїв в EZVIZ хмару

3.3 Результати тестування системи корпоративного відеоспостереження

З метою тестування системи корпоративного відеоспостереження використано продукти компанії HikVision iVMS-4200 – для персональних комп’ютерів [25,26], iVMS-4500 - для мобільних пристроїв [27], а також EZVIZ Studio для користування хмарними сервісами відеоспостереження.

Основна панель програми iVMS-4200 зображена на рисунку 3.8.

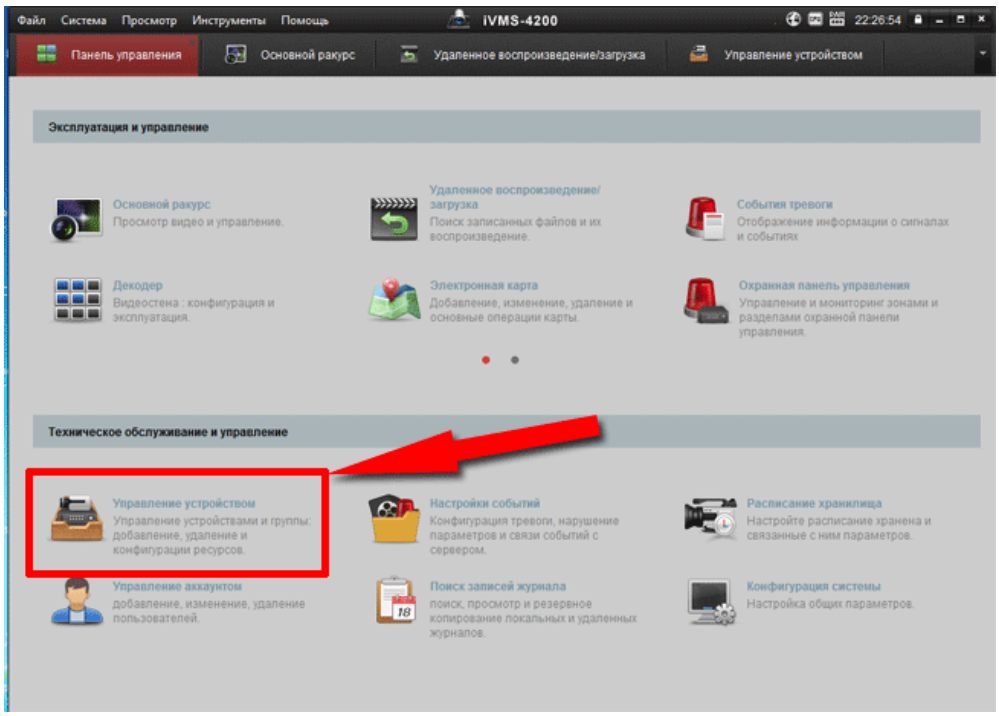

Рисунок 3.8 – Інформаційна панель iVMS-4200

Для добавлення пристроїв (камер, відео реєстраторів тощо) в ситему відео моніторингу потрібно здійснити наступні кроки.

На головній інформаційній панелі, натискаємо «Додати» і вводимо: псевдонім - будь-яка назва; адресу - постійний IP адреса, який вам дав провайдер; порт - залишаємо 8000; користувач - admin; пароль - ваш пароль на камеру або реєстратор, який вводиться при первинній активації пристрою.

Завершуючи процес, натискаємо кнопку «Додати» внизу вікна, де вводили дані (рисунок 3.9).

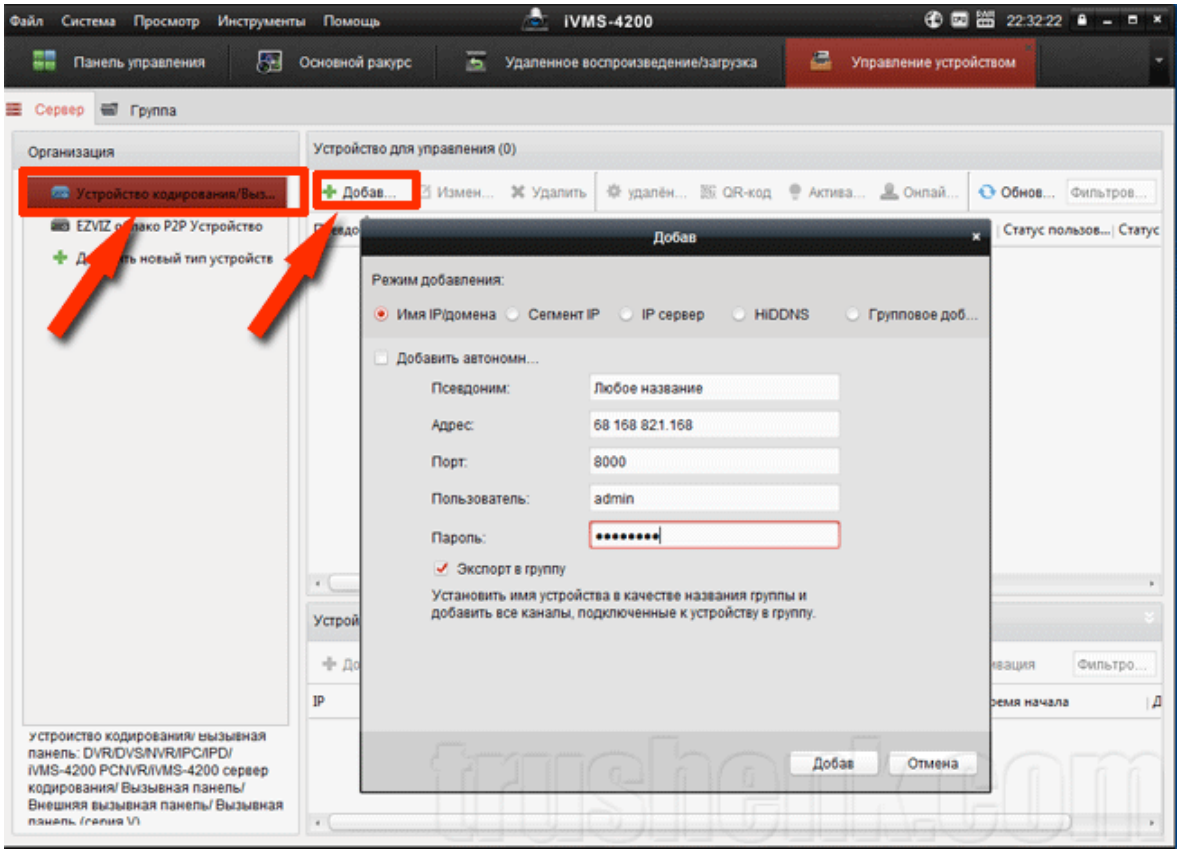

Рисунок 3.9 – Добавлення пристроїв до панелі управління

Після цього повертаємося в Панель управління і натискаємо «Основний ракурс»

Нажимаємо на клавіші, показані стрілками (спочатку на нижню, потім на верхню) і у нас, якщо все зроблено правильно, починає показувати камера в реальному часі (рисунок 3.10).

А щоб подивитися запис, необхідно в Панелі управління натиснути «Віддалене відтворення». Вибираємо потрібну дату і двічі натискаємо на потрібну камеру (рисунок 3.11).

Зауважимо, що можливості програми iVMS-4200 набагато ширші, ніж просто віддалений перегляд камер відеоспостереження.

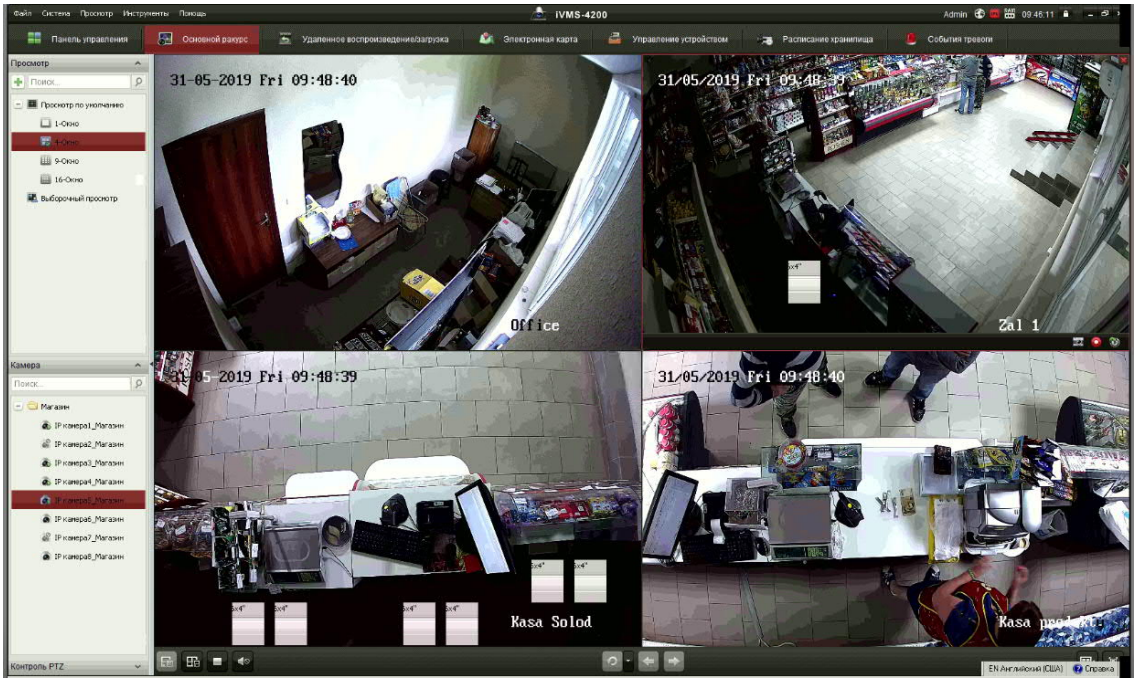

Рисунок 3.10 – Перегляд камер в реальному часі

Вона також дозволяє робити настроювання різних параметрів IP камер і реєстраторів (якщо ви знаєте пароль на вхід цих пристроїв), а також працює з охоронними і панелями виклику.

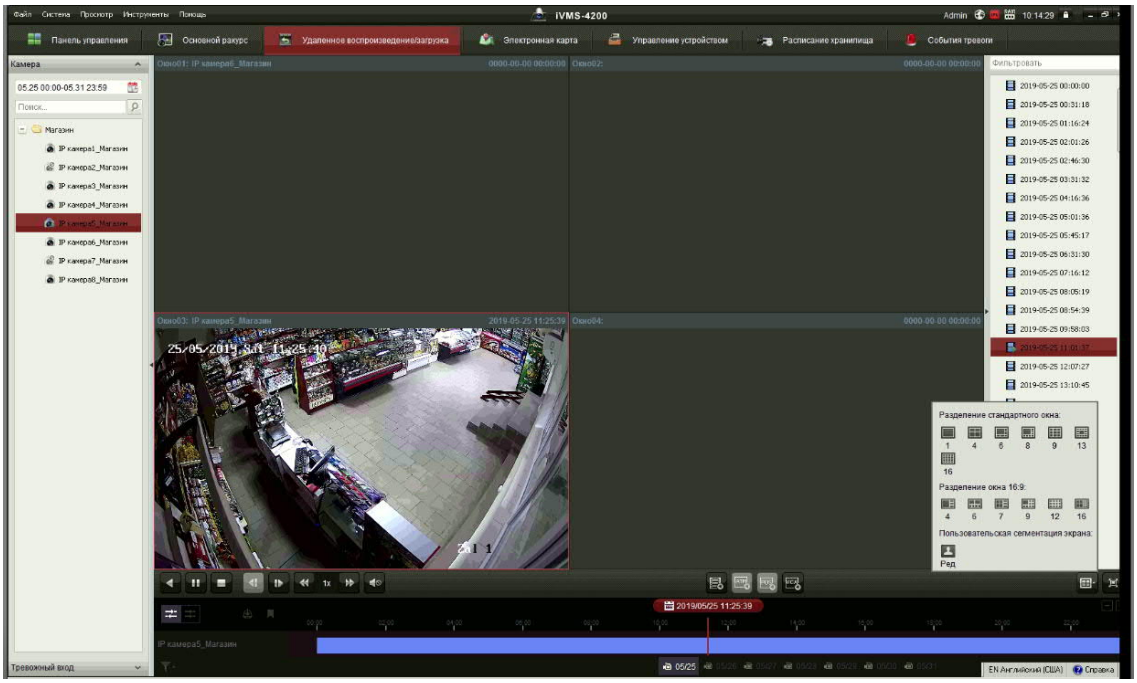

Рисунок 3.11 – Віддалений перегляд відеоархіву

За допомогою камери Hikvision і безкоштовного мобільного додатку IVMS 4500, розробленого фахівцями Hikvision Digital Technology, завжди можна бути в курсі того, що відбувається на підконтрольній території.

Для додавання пристрою у мобільний додаток IVMS-4500, потрібно встановити його з Play Market (для Android) або App Store (для iOS), запускаємо його і бачимо меню програми. Додаємо камеру або реєстратор у вкладці "Пристрої" (рисунок 3.12).

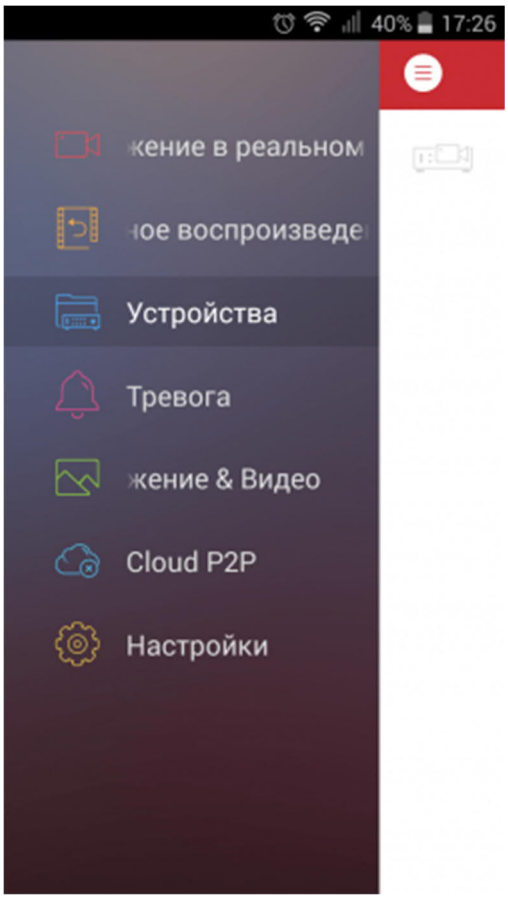

Рисунок 3.12 – Добавлення пристрою у мобільному додатку IVMS-4500

Для цього у вікні натискаємо на кнопку "+" і вибираємо ручне додавання (рисунок 3.13).

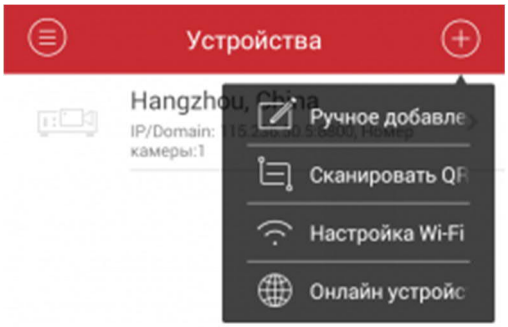

Рисунок 3.13 – Ручне добавлення пристрою відеоспостереження

У вікні нового пристрою вводимо його параметри (рисунок 3.14).

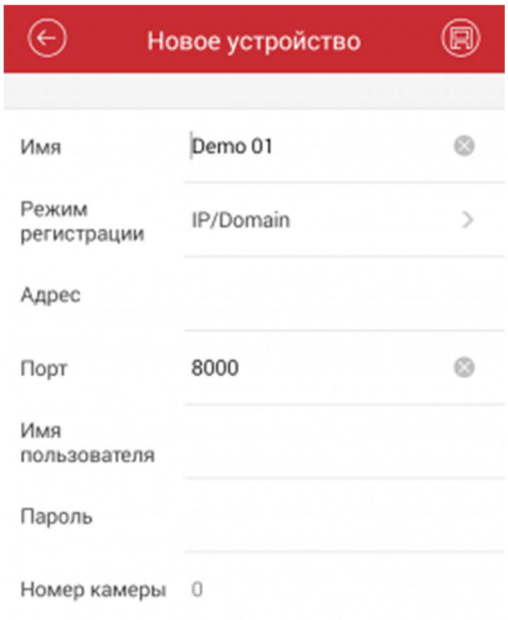

Рисунок 3.14 – Параметри нового пристрою

Бажане ім'я пристрою, наприклад, "Зал 1", у полі "Адреса"- IP-адресу (статичну), у полі "Порт" вводимо порт, який "прокинутий" на роутері (він же порт пристрою), у полі "Ім'я користувача" - логін (стандартно - "admin"),у полі "Пароль" вводимо пароль, який заданий камері чи реєстратору під час активації.

Якщо все було зроблено правильно, то потрібно натиснути на кнопку "Почати показ у реальному часі". У вкладці, що відкрилася, ви побачите відео з камери (рисунок 3.15).

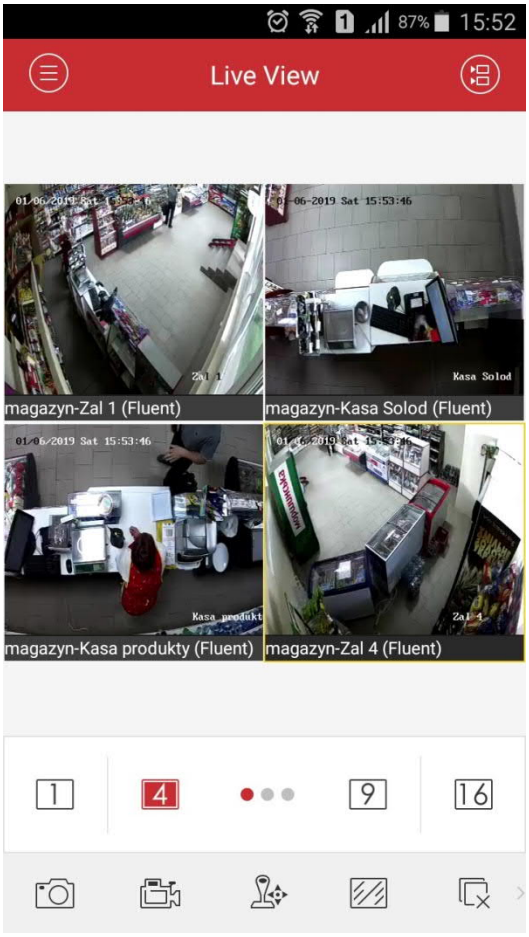

Рисунок 3.15 – Перегляд камер у реальному часі

При подвійному натисканні на зображення воно розгорнеться на весь екран.

Окрім перегляду відео у реальному часі, додаток має ще кілька функцій, зручних для користувача, наприклад, перегляд архіву. Увійти до віддаленого відтворення можна через головне меню програми.

Для перегляду архіву через мобільний пристрій попередньо потрібно налаштувати камеру або реєстратор на запис в інтерфейсі самого пристрою, через ПЗ додатки IVMS 4200 або в інтерфейсі браузера на комп'ютері. Якщо ви вже зробили це, то у вкладці "Віддалене відтворення" під час вибору потрібної вам камери, відобразиться архів записів з цієї камери (рисунок 3.16).

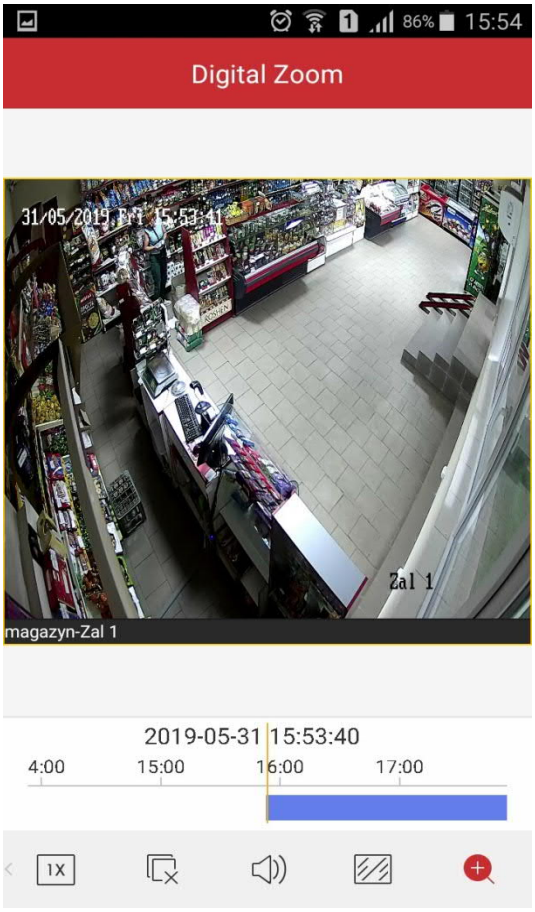

Рисунок 3.16 – Перегляд відеоархіву

За допомогою пересування доріжки відеозапису вправо або вліво ви зможете переглядати запис за певний відрізок часу.

Для перегляду камери через хмару EZVIZ у випадку, якщо немає статичної IP-адреси потрібно відкрити вкладку Cloud P2P (рисунок 3.17)

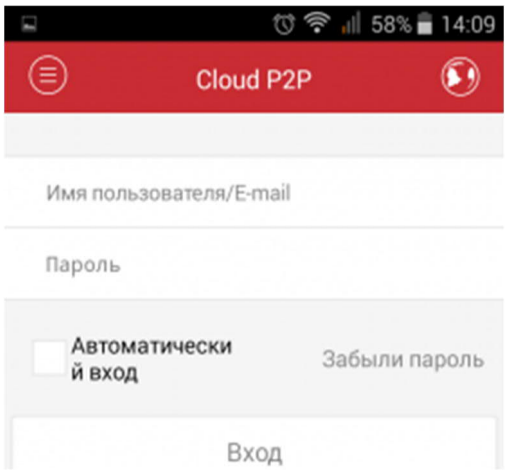

Рисунок 3.17 – Робота в хмарному сервісі

У цьому розділі «Налаштування» знаходяться додаткові налаштування: захист паролем, статистика трафіку, налаштування Wi-Fi та інше. Натиснувши на кнопку "Допомога" можна переглянути інструкцію використання програми англійською мовою (рисунок 3.18).

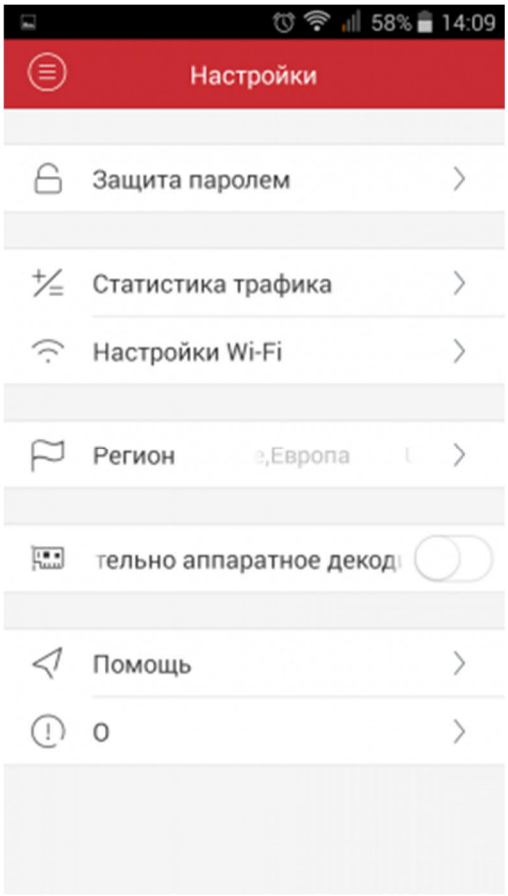

Рисунок 3.18 – Додаткові налаштування IVMS-4500

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

В даному розділі дипломного проекту проводиться економічне обґрунтування доцільності впровадження системи корпоративного відеоспостереження на основі моделі SaaS. Зокрема, здійснюється розрахунок витрат на розробку системи, експлуатаційних витрат, ціни споживання проектного рішення. В заключній частині визначаються показники економічної ефективності запропонованого рішення, обґрунтовуються відповідні висновки [28-30].

Розроблена система корпоративного відеоспостереження на основі SaaS моделі призначена для моніторингу продуктового магазину і характеризується підвищеною надійністю та безпекою, можливістю віддаленого доступу до локальної системи та моніторингу через хмарний сервіс Ezviz .

4.1 Розрахунок витрат на розробку системи відеоспостереження

Витрати на розробку і впровадження системи відеоспостереження (К) включають:

$$К = К_1, + К_2$$

де $К_1$ - витрати на розробку та впровадження системи, грн.;

$К_2$ - витрати на відлагодження і тестування програмного забезпечення моніторингу, грн.

Витрати на розробку і впровадження системи відеоспостереження включають:

– витрати на оплату праці розробників ($B_{ОП}$);

– витрати на відрахування у спеціальні державні фонди ($Вф$);

– витрати на покупні вироби ($Пв$);

– витрати на придбання спецобладнання для проведення експериментальних робіт ($Об$);

– накладні витрати ($Н$);

– інші витрати ($Ів$).

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт у людино-днях та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту, студент-дипломант, консультант техніко-економічного розділу.

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

№ п/п	Посада виконавців	Місячний оклад, грн.
1	Керівник ДП, викладач	5470
2	Консультант техніко-економічного розділу, Доцент	6026
3	Студент	1200

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} , \quad (4.1)$$

де n_{ij} – чисельність розробників *i*-ої спеціальності *j*-го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником *i*-ої спеціальності *j*-го тарифного розряду, год;

C_{ij} – годинна ставка працівника *i*-ої спеціальності *j*-го тарифного розряду, грн.,

Середньо годинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_{i}}, \qquad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника *i*-ої спеціальності *j*-го тарифного розряду, грн.;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (0,58);

$РЧ_i$ - місячний фонд робочого часу працівника *i*-ої спеціальності *j*-го тарифного розряду, год. (приймаємо 168 год.).

Результати розрахунку записують до таблиці 4.2.

Таблиця 4.2 - Розрахунок витрат на оплату праці

№ п/п	Посада виконавців	Час розробки, год	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн.
1	Керівник ДП, викладач	16	51,44	823,04
2	Консультант техніко-економічного розділу, Доцент	2	51,44	102,88
3	Студент	144	8,33	1199,52
Разом				2125,44

Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних

плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

$$B_{\Phi} = \frac{20,5}{100} \cdot 2125,44 = 435,72 \text{ грн.}$$

У таблиці 4.3 наведений перелік купованих виробів і розраховані витрати.

Таблиця 4.3- Розрахунок витрат на матеріали та комплектуючі

№ п/п	Найменування купованих виробів	Одиниця виміру	Ціна, грн	Кількість куповани х виробів	Сума , грн	Транспортні витрати (10% від суми)	Загальна сума, Грн.
1	Папір (формат А4)	Уп	84,0	2	168,0	16,8	184,8
2	Ручка кулькова	Шт	15,0	2	30,0	3,0	33,0
3	Олівець простий	Шт.	10,0	2	20,0	2,0	22,0
4	Флеш-пам’ять	Шт.	100,0	1	100,0	10,0	110,0
5	Зошит, 96 арк	Шт.	15,50	2	31,0	3,10	34,10
6	Тонер для принтера	Уп	85	1	85	8,5	93,5
Разом							477,40

Витрати на використання комп’ютерної техніки включають витрати на амортизацію комп’ютерної техніки, витрати на користування програмним забезпеченням, витрати на електроенергію, що споживається комп’ютером. За даними обчислювального центру ТНЕУ для комп’ютера типу IBM PC/ATX вартість години роботи становить 5,32 грн. Середній щоденний час роботи на комп’ютері – 2 години. Розрахунок витрат на використання комп’ютерної техніки приведений в таблиці 4.4.

В процесі досліджень використовувалось спеціальне обладнання –IP камери, выдеореєстратор, то відповідні витрати розраховуються за структурою, приведеною в таблиці 4.5.

Таблиця 4.4- Розрахунок витрат на використання комп'ютерної техніки

№ п/п	Назва етапів робіт, при виконанні яких використовується комп'ютер	Час використання комп'ютера, год.	Витрати на використання комп'ютера грн.
1	Проведення досліджень та оформлення їх результатів	60	319,2
2	Оформлення техніко-економічного розділу	8	42,56
4	Оформлення ДП	12	63,84
Разом		80	425,6

Таблиця 4.5- Розрахунок витрат за статтею "Спецобладнання для наукових (експериментальних) робіт"

Види робіт на спецобладнанні	Кількість годин роботи	Вартість 1год. роботи (грн.)	Сума (грн.)
Відеокамери	8	125,16	1001,28
Відеореєстратор	8	200	1600
Маршрутизатор	4	100	400
Разом			3001,28

Накладні витрати проектних організацій включають три групи видатків: витрати на управління, загальногосподарські витрати, невиробничі витрати. Вони розраховуються за встановленими відсотками до витрат на оплату праці. Середньостатистичний відсоток накладних витрат приймемо 150% від заробітної плати:

$$H = 1{,}5 \cdot 2125{,}44 = 3188{,}16 \text{ (грн.)}$$

Інші витрати є витратами, які не враховані в попередніх статтях. Вони становлять 10% від заробітної плати:

$$I = 2125{,}44 \cdot 0{,}1 = 212{,}54 \text{ (грн.)}$$

Витрати на розробку системи відеоспостереження складають:

$$K_1 = B_{ОП} + B_Ф + B_{ПВ} + H + I$$

$$K_1 = 2125{,}44 + 435{,}72 + 477{,}40 + 318{,}16 + 212{,}54 = 6439{,}26 \text{(грн.)}$$

Витрати на відлагодження і дослідну експлуатацію програмного продукту визначаємо за формулою:

$$K_2 = S_{м.г.} \cdot t_{від} \qquad (4.2)$$

де $S_{м.г.}$ - вартість однієї машино-години роботи ПК, грн./год.;

$t_{від}$ - комп'ютерний час, витрачений на відлагодження і дослідну експлуатацію створеного програмного продукту, год.

Загальна кількість днів роботи на комп'ютері дорівнює 40 днів. Середній щоденний час роботи на комп'ютері – 2 години. Вартість години роботи комп'ютера дорівнює 5,32 грн. Тому

$$K_2 = 5{,}32 \cdot 80 = 425{,}6 \text{ грн.}$$

На основі отриманих даних складаємо кошторис витрат на розробку програмного забезпечення.

4.2 Визначення експлуатаційних витрат

Для оцінки економічної ефективності розроблюваної комп'ютерної системи слід порівняти його з аналогом, тобто існуючою комп'ютерною системою ідентичного функціонального призначення.

Експлуатаційні одноразові витрати по комп'ютерній системі і аналогу включають вартість підготовки даних і вартість роботи комп'ютера (за час дії програми):

Таблиця 4.6 - Кошторис витрат на розробку системи відеоспостереження

№ п/п	Найменування витрат	Сума витрат, грн.
1	Витрати на оплату праці	2125,44
2	Відрахування у спеціальні державні фонди	435,72
3	Витрати на куповані вироби	477,40
4	Витрати на використання спеціального обладнання	3001,29
5	Накладні витрати	3188,16
6	Інші витрати	212,54
7	Витрати на відлагодження і дослідну експлуатацію системи відеоспостереження	425,60
Разом		9866,15

$$E_{\text{П}} = E_{1\text{П}} + E_{2\text{П}},$$

де E_n - одноразові експлуатаційні витрати на систему відеоспостереження (аналог), грн.;

E_{1n} - вартість підготовки даних для експлуатації системи відеоспостереження (аналогу), грн.;

E_{2n} - вартість роботи комп'ютера для виконання проектного рішення (аналогу), грн.

Річні експлуатаційні витрати B_{en} визначаються за формулою:

$$B_{ЕП} = E_{П} * N_{П},$$

де N_n - періодичність експлуатації ПЗ (аналогу), раз/рік.

Вартість підготовки даних для роботи на комп'ютері визначається за формулою:

$$E_{1П} = \sum_{l=1}^{n} n_i t_i c_i,$$

де i - категорії працівників, які приймають участь у підготовці даних (i=1,2,...n);

n_i - кількість працівників і-ої категорії, осіб;

t_i - трудомісткість роботи співробітників і-ої категорії по підготовці даних, год.;

c_i - середнього годинна ставка працівника і-ої категорії з врахуванням додаткової заробітної плати, що знаходиться із співвідношення:

$$c_i = \frac{c_i^0 (1+b)}{m},$$

де c_i^0 - основна місячна заробітна плата працівника і-ої категорії, грн.;

b - коефіцієнт, який враховує додаткову заробітну плату (приймемо 0,58);

m - кількість робочих годин у місяці, год.

Для роботи з даними як для проектного рішення так і аналогу потрібен один працівник на 0,5 ставки, місячна заробітна плата якого складає: с° = 4100 грн. Тоді:

$$c_1 = \frac{4100(1+0,58)}{22*8} = 36,81 \text{ грн/год}$$

Трудомісткість підготовки даних для проектного рішення складає 1 год., для аналога 1,5 год.

Таблиця 4.7- Розрахунок витрат на підготовку даних та реалізацію проектного рішення на комп'ютері

№	Час роботи співробітників, год.	Середньогодинна заробітна плата, грн./год.	Витрати , грн.
	Проектне рішення		
1	1	36,81	36,81
	Аналог		
1	1,5	36,81	55,22

Витрати на експлуатацію комп'ютера визначається за формулою:

$$E_{2П} = t * S_{МГ}$$

де t - витрати машинного часу для реалізації проектного рішення (аналогу), год.;

$S_{МГ}$ - вартість однієї години роботи комп'ютера, грн./год.

E_{2n}= 1· 5,32 = 5,32 грн.; E_{2a}=1,5·5,32 = 7,98 грн.

E_n=36,81+5,32=42,13 грн. ; E_a=55,22+7,98 = 63,20 грн.

B_{en}= 42,13*55=2317,15 грн. ; B_{ea}=63,20*55=3476,00 грн.

4.3 Розрахунок ціни споживання проектного рішення

Ціна споживання - це витрати на придбання і експлуатацію проектного рішення за весь строк його служби:

$$Ц_{С(П)} = Ц_{П} + B_{(E)NPV},$$

де $Ц_п$ - ціна придбання проектного рішення, грн.:

$$Ц_{П} = K(1+\frac{П_{Р}}{100}) + K_0 + K_к$$

де $К$ - кошторисна вартість;

$Пр$ - рентабельність;

$К_о$ - витрати на прив'язку та освоєння проектного рішення на конкретному об'єкті, грн.;

$К_к$ - витрати на доукомплектування технічних засобів на об'єкті, грн.

$$Ц_п = 9866{,}15 \cdot (1+0{,}3) = 12826 \text{ грн.}$$

Вартість витрат на експлуатацію проектного рішення (за весь час його експлуатації), грн.:

$$B_{епрv} = \sum_{t=0}^{T} \frac{B_{еП}}{(1+R)^t}$$

де $В_{еп}$ - річні експлуатаційні витрати, грн.;

$Т$ - строк служби проектного рішення, років;

R - річна ставка проценту банку.

$$B_{е\text{пр}v} = \sum_{t=1}^{5} \frac{2317{,}15}{(1+0{,}23)^t} = 6489{,}07 \text{ грн.}$$

$$B_{е\text{пр}v} = \sum_{t=1}^{5} \frac{3476{,}00}{(1+0{,}23)^t} = 9734{,}38 \text{ грн.}$$

Тоді ціна споживання проектного рішення дорівнюватиме:

$Ц_{сп}$ = 10226,00+6489,07=16715,07 грн.

Аналогічно визначається ціна споживання для аналогу:

$Ц_{са}$ = 12000+9734,38=21734,38 грн.

4.4 Визначення показників економічної ефективності

Економічний ефект в сфері проектування рішення:

$$E_{ПР} = Ц_{П} - Ц_{А}$$

$E_{ПР}$ =10226 – 12000 = 1774 грн.

Річний економічний ефект в сфері експлуатації:

$$E_{КС} = B_{ЕА} - B_{ЕП}$$

$E_{кс}$=3476-2317,15= 1158,85 грн.

Додатковий економічний ефект у сфері експлуатації:

$$\Delta E_{екс} = \sum_{t=1}^{T} E_{екс}(1+R)^{T-t}$$

$$\Delta E_{екс} = \sum_{t=1}^{5} 1158{,}85(1+0{,}23)^{5-t} = 3245{,}30 \text{ грн.}$$

Сумарний ефект складає:

$$E = E_{пр} + \Delta E_{екс} = 1774 + 3245{,}30 = 5019{,}3 \text{ грн.}$$

В даному розділі проведено розрахунок витрат на розробку проектного рішення. Здійснено порівняння з існуючим аналогом, і цим показано, що дане проектне рішення має переваги в порівнянні з аналогами. Згідно проведеного економічного обґрунтування дане проектне рішення є конкурентноздатним.

Таблиця 4.8 - Показники економічної ефективності проектного рішення

№	Найменування	Одиниці вимірювання	Значення показників	
			Базовий варіант	Новий варіант
1	Капітальні вкладення	грн.	-	9866,15
2	Ціна придбання	грн.	12000	12826,00
3	Річні експлуатаційні витрати	грн.	3476,00	2317,15
4	Ціна споживання	грн.	21734,38	16715,07
5	Економічний ефект в сфері проектування	грн.	-	1774,00
6	Економічний ефект в сфері експлуатації	грн.	-	1158,85
7	Додатковий ефект в сфері експлуатації	грн.	-	3245,30
8	Сумарний ефект	грн.	5019,30	

Крім того, отримано економічний ефект у розмірі 5019,30 грн. і тому розробка корпоративної системи відеоспостереження є економічно доцільною.

ВИСНОВКИ

В бакалаврській роботі розроблено корпоративну систему відеоспостереження. На даний час є можливість інтегрувати її в загальні інформаційні системи, в тому числі і з системами звичайного телебачення, обробляти і передавати сигнал на будь-які відстані через Інтернет, використовувати хмарні технології (SaaS) і використовувати цю інформацію в інтелектуальних системах, які здатні самостійно приймати оптимальні рішення щодо забезпечення безпеки об'єктів. Зокрема:

1. Проведено огляд основних компонентів систем корпоративного відеоспостереження. Показано переваги та недоліки аналогових, цифрових та IP-камер. Розглянуто основні характеристики камер: об’єктиви, кут огляду, роздільну здатність, чутливість. Обгрунтовано доцільність використання IP-камер з широким кутом огляду з високою світловою чутливістю для торгових залів.

2. Розглянуто середовища передачі відеосигналів, їх переваги та недоліки. Також, обґрунтовано доцільність використання різних каналів в залежності від середовища використання та вимог до безпеки.

3. Проаналізовано використання віддаленого доступу до системи корпоративного відеоспостереження через мережу Інтеренет. А також, обґрунтовано доцільність використання хмарних технологій на основі моделы SaaS, для забезпечення надійності, безпеки, гнучкості, та можливості інтеграції з іншими об’єктами відеоспостереження організації. Зокрема, доступ до он-лайн перегляду і відеоархіву на NVR або NAS и бекап відеоархіву в хмару.

4. Розроблено логічну структуру системи корпоративного відеоспостереження, зокрема встановлено вимоги використання технології – PlugNPlay, мультиплатформеності, розмежування прав доступу, інтеграцію з іншими інформаційно-вимірювальними системами організації.

5. Розроблено політику безпеки захисту корпоративного хмарного відеоспостереження, зокрема встановлено вимоги до запобігання механічних силових дій, електромагнітного впливу, керуючих впливів на апаратні пристрої системи відеоспостереження, а також захист від втручання в програмне забезпечення та вплив на відео архіви. Окремо виділено вимоги до безпеки використання хмарних сервісів.

6. Проведено технічну реалізацію системи корпоративного відеоспостереження. Зокрема, визначено кількість камер та їх розташування, їх моделі, обґрунтовано вибір відео реєстратора та живлення для системи. Здійснено монтаж та первинне налаштування апартного та програмного забезпечення, а також налаштування віддаленого доступу через мережу Інтернет.

7. Налаштовано використання хмарного сервісу EZVIZ для системи відеоспостереження торгового залу продуктового магазину.

8. Проведено тестування використання системи. Використано програмне забезпечення компанії HikVision iVMS-4500 та мобільний додаток iVMS-4200 для налаштування та віддаленого доступу до системи відеоспотсереження, моніторингу та перегляду відеоархіву.

6. Проведено розрахунок витрат на розробку проектного рішення. Здійснено порівняння з існуючим аналогом, і цим показано, що дане проектне рішення має переваги в порівнянні з аналогами. Згідно проведеного економічного обґрунтування дане проектне рішення є конкурентноздатним. Крім того, отримано економічний ефект у розмірі 3019,30 грн. і тому розробка і впровадження системи корпоративного відеоспостереження на основі SaaS моделі є економічно доцільним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кашкаров А.П. Системы видеонаблюдения: практикум / А.П. Кашкаров. – Ростов-на-Дону.: Феникс, 2014. 82 с.
2. Основы сетевого виденаблюдения [Електронний ресурс].–2017.– 35с. – Режим доступу: https://www.secfocus.ru/shop/books/19000.htm.
3. Що таке ТВЛ? [Електронний ресурс] /Hikvisoin - 2018. – Режим доступу: https://hikvision.org.ua/ua/articles/shcho-take-tvl.
4. Kanazawa Y. Wide baseline matching using triplet vector descriptor / Y.Kanazawa, K.Uemura // Proc. 17th British Machine Vision Conf. – Edinburgh (U.K). - Vol. I. – 2016. - P. 267-276.
5. Shi J. Good features to track / J.Shi, C.Tomasi // IEEE conference on computer vision and pattern recognition. – Seattle (USA). - 2014. – P.544-567.
6. Организация видеонаблюдения через Интернет [Електронний ресурс].– Режим доступу: http://bookash.pro/ru/book/78295/sistemy.
7. Дамьяновски В. Библия видеонаблюдения / В. Дамьяновски .– Security Focus, 2019.– 470 с.
8. Хмарна піраміда: IAAS, PAAS і SAAS. [Електронний ресурс]. Режим доступу: https://gigacloud.ua/blog/navchannja/hmarna-piramida-iaas-paas-i-saas.
9. Облачное видеонаблюдение: что должен знать каждый? [Електронний ресурс] / Интемс – 2017. – Режим доступу: https://habr.com/ru/company/intems/blog/320790/
10. Облачная служба. [Електронний ресурс]. – Режим доступу: https://www.ezvizlife.com/ru/p/cloud-service.
11. Скворцов А.В. Триангуляция Делоне и её применение / А.В. Скворцов. – Томск: Изд-во Том. ун-та, 2012.–128 с.

12. Реклейтис Г. Оптимизация в технике / Г.Реклейтис, А.Рейвиндран, К.Рэгсдел .– Т.1,2., 1986. – 672 с.

13. Цыпкин Я.З. Основы теории автоматических систем: учеб. пособие для вузов./ Я.З.Цыпкин – М.: Наука, 1977. – 560с.

14. Томашевський В.М. Моделювання систем./ В.М.Томашевський – К: Видавнича група BHV, 2005. – 352с.

15. Pratt W. Digital image processing / W. Pratt - New York, Chichester, Brisbane, Torc: A Wiley-interscience publication, John Wiley and sons, 2008. – 541p.

16. Облачный (IaaS/SaaS) сервис-провайдер и проблемы безопасности: три шага на пути предотвращения угроз [Електронний ресурс] / SecurityLab – 2017. – Режим доступу: https://www.securitylab.ru/blog/company/IT-GRAD/263444.php.

17. Georgis N. On the correspondence problem for wide angular separation of non-coplanar points / N.Georgis, M.Petrou, J.Kittler // Image and vision computing. - 2008. - Vol. 16. - P. 35-41.

18. Lourakis M. Matching disparate views of planar surfaces using projective invariants / M. Lourakis, S.Halkidis // Image and Vision computing. – 2010. - Vol. 18. - P. 673-683.

19. Lowe D. Distinctive image features from scale-invariant keypoints / D.Lowe // International journal of computer vision.-2014. - Vol.8. – P.167-176.

20. Відеоспостереження в супермаркетах [Електронний ресурс] / HikVision – 2017. – Режим доступу: https://hikvision.org.ua/ua/articles/videosposterezhennya-v-supermarketah.

21. Доступ до пристрою з інтернету [Електронний ресурс] / HikVision – 2016. – Режим доступу: https://hikvision.org.ua/ua/articles/dostup-do-prystroyu-z-internetu

22. Мобільні додатки Hikvision. Тонкощі роботи з Ezviz. [Електронний ресурс] / HikVision – 2017. – Режим доступу:

https://hikvision.org.ua/ua/articles/mobilni-dodatky-hikvision-tonkoshchi-roboty-z-ezviz.

23. Як підключити IP-камеру або реєстратор до хмарного сервісу EZVIZ. [Електронний ресурс] / HikVision – 2017. – Режим доступу: https://hikvision.org.ua/ua/articles/yak-pidklyuchyty-ip-kameru-abo-reyestrator-do-hmarnogo-servisu-ezviz.

24. Как установить верификационный код для сервиса Ezviz? [Електронний ресурс] / HikVision – 2017. – Режим доступу: https://hikvision.org.ua/ru/articles/kak-ustanovit-verifikacionnyy-kod-dlya-servisa-ezviz.

25. Hikvision iVMS-4200 — установка и настройка программы [Електронний ресурс].–2017.– Режим доступу: https://trushenk.com/hikvision-ivms-4200-ustanovka-i-nastrojka-programmy.html.

26. Як налаштувати права доступу на пристроях Hikvision? [Електронний ресурс] / HikVision – 2017. – Режим доступу: https://hikvision.org.ua/ua/articles/yak-nalashtuvaty-prava-dostupu-na-prystroyah-hikvision.

27. Як налаштувати та використовувати мобільний додаток IVMS 4500 для камер Hikvision [Електронний ресурс] / HikVision – 2017. – Режим доступу: https://hikvision.org.ua/ua/articles/yak-nalashtuvaty-ta-vykorystovuvaty-mobilnyy-dodatok-ivms-4500-dlya-kamer-hikvision.

28. Смерека В.В. Корпоративне хмарне відеоспостереження на основі SAAS моделі / В.В.Смерека // Тези доповідей науково-практичної конференції молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі». - Тернопіль: ТНЕУ. - 2019. - С. 14.

29. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та

мережі» / О.М. Березький, Л.О.Дубчак, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2017. – 60 с.

30. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп'ютерна інженерія/ І.Р. Паздрій – Тернопіль: ТНЕУ, 2014. – 37 с.