

ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
Навчально-науковий інститут економіки, управління, права та
інформаційних технологій
Кафедра інформаційних систем та технологій

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти бакалавр

на тему: **«Проектування ІР-системи відеоспостереження на підприємстві»**

Виконав: здобувач вищої освіти
за освітньою програмою
Інформаційні управляючі системи
спеціальності 126 Інформаційні
системи та технології
ступеня вищої освіти бакалавр
групи 126ІСТ_бд_2021
Колесніченко Антон Артемович
Керівник: Одарущенко Олег
Миколайович
Рецензент: Муравльов Володимир
Вячеславович

Полтава – 2025 року

ВСТУП

Актуальність. У сучасному світі системи відеоспостереження є невід'ємною частиною забезпечення безпеки комерційних об'єктів, зокрема офісів, що працюють із конфіденційною інформацією. За даними аналітичних звітів [1, 2], світовий ринок систем відеоспостереження у 2024 р. досяг обсягу 50 млрд \$, а в Україні попит на IP-системи відеоспостереження зростає на 15-20% щорічно. Особливо актуальними є IP-системи, які забезпечують високу якість зображення, віддалений доступ, інтеграцію з іншими охоронними системами та можливості масштабування [3]. В Україні, за оцінками SecurityMarket, у 2024 р. частка IP-систем на ринку безпеки склала 65%, що свідчить про перехід до цифрових технологій у сфері відеоспостереження [4].

Однак багато існуючих систем відеоспостереження мають обмеження: недостатнє покриття критичних зон, низька роздільна здатність, складність інтеграції з охоронними системами чи відсутність сучасних функцій, таких як відеоаналітика та хмарне зберігання [5]. Це створює потребу в розробці IP-систем відеоспостереження, які б відповідали сучасним вимогам безпеки, забезпечували надійність, зручність управління та економічну ефективність. Розробка IP-системи відеоспостереження для офісу ТОВ «Інноваційні Технології», орієнтованої на захист конфіденційної інформації, контроль доступу та підтримку масштабування, є актуальним завданням, що сприяє підвищенню безпеки підприємства та зниженню ризиків.

Мета кваліфікаційної роботи полягає в розробці IP-системи відеоспостереження для офісу ТОВ «Інноваційні Технології» з використанням сучасних технологій, що забезпечує автоматизацію процесів моніторингу, захист даних і економічну ефективність.

Відповідно до мети роботи необхідно вирішити наступні завдання:

- 1) провести аналіз предметної галузі, сучасних технологій, вимог до IP-систем відеоспостереження та порівняння технічних рішень;

2) спроектувати архітектуру IP-системи відеоспостереження, включаючи розміщення обладнання, конфігурацію мережі та інтеграцію з іншими системами безпеки;

3) реалізувати IP-систему відеоспостереження, включаючи налаштування обладнання, організацію доступу, а також провести економічний аналіз її ефективності та розробити рекомендації щодо масштабування і модернізації.

Об'єкт дослідження – процеси проектування та впровадження IP-систем відеоспостереження для забезпечення безпеки комерційних об'єктів.

Предмет дослідження – проектування та розробка IP-системи відеоспостереження для офісу ТОВ «Інноваційні Технології» з використанням сучасного обладнання та програмного забезпечення.

Методи досліджень – дослідження базуються на методах системного аналізу, порівняльного аналізу технічних рішень, проектування мережевих систем, конфігурування обладнання, а також техніко-економічного аналізу для оцінки ефективності системи.

Інформаційна база – Інтернет-ресурси, наукові статті, технічна документація на обладнання (Hikvision, D-Link, APC), стандарти безпеки, а також статистичні дані про ринок систем відеоспостереження та тенденції розвитку охоронних технологій.

Практична значущість – розроблена IP-система відеоспостереження забезпечує повне покриття критичних зон офісу, захист конфіденційної інформації та зручний віддалений доступ.

Результати роботи апробовані в рамках наукової конференції здобувачів вищої освіти за результатами науково-дослідної роботи у 2024-2025 рр.

Структура кваліфікаційної роботи логічно пов'язана з задачами досліджень і містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел. Загальний обсяг текстової частини кваліфікаційної роботи складає 48 сторінок формату А4. Вона містить 12 рисунків і 9 таблиць.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ТА АНАЛІЗ СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

1.1 Аналіз об'єкта дослідження і системи безпеки підприємства

Об'єктом дослідження є офісне приміщення компанії ТОВ «Інноваційні Технології», розташоване на першому поверсі триповерхової адміністративної будівлі у м. Київ. Загальна площа приміщення становить близько 250 м². Компанія займається наданням послуг у сфері інформаційних технологій: проектуванням серверної інфраструктури, розробкою програмного забезпечення, впровадженням рішень у галузі інформаційної безпеки, хмарних технологій та технічної підтримки. ТОВ «Інноваційні Технології» обслуговує понад 80 корпоративних клієнтів у межах України та Європейського Союзу, зокрема з промислового, фінансового та освітнього секторів. У діяльності підприємства особливе місце займає обробка та зберігання конфіденційної інформації клієнтів, а також підтримка функціонування критично важливої інфраструктури, тому забезпечення фізичної безпеки офісу є стратегічним пріоритетом.

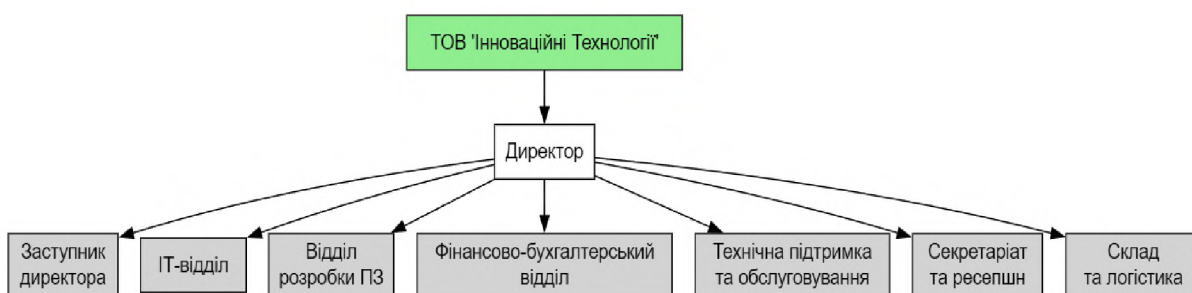


Рисунок 1.1 – Організаційно-штатна структура ТОВ «Інноваційні Технології»

Організаційно-штатна структура підприємства є лінійно-функціональною (рис. 1.1) і включає такі основні підрозділи:

1. Адміністративно-управлінський персонал: директор, заступник директора, керівник ІТ-відділу, головний бухгалтер.

2. IT-відділ: системні адміністратори, мережеві інженери, фахівці з безпеки, DevOps-інженери.

3. Відділ розробки ПЗ: програмісти front-end і back-end, UI/UX-дизайнери, тестувальники.

4. Фінансово-бухгалтерський відділ: бухгалтерія, каса, економіст.

5. Технічна підтримка та обслуговування: helpdesk, спеціалісти з монтажу обладнання.

6. Склад та логістика: облік техніки, відправлення, зберігання.

7. Секретаріат та ресепшн.

Загальна кількість штатних працівників становить 38 осіб. Частина працівників працює віддалено, однак серверна інфраструктура, бухгалтерія, керівництво та служба підтримки працюють виключно з офісу. Саме тому важливо забезпечити відеоконтроль за критичними приміщеннями.

З економічної точки зору, ТОВ «Інноваційні Технології» демонструє стабільне зростання. За даними бухгалтерської звітності за 2024 р. частка витрат на обслуговування інфраструктури, включно з безпековими технологіями, становила 12% від загального бюджету операційної діяльності.

Стабільність фінансових показників, розширення клієнтської бази та підвищені вимоги до інформаційної безпеки створюють потребу в реалізації сучасної IP-системи відеоспостереження, яка забезпечить як зовнішній, так і внутрішній контроль усіх зон доступу та переміщення. Згідно з планом приміщення (додаток А), у нього ведуть два входи: основний (для співробітників та відвідувачів) та службовий (для персоналу й технічного обслуговування). Основні приміщення, що потребують відеоконтролю:

- касова кімната (№5);
- серверна (№6);
- бухгалтерія (№9);
- склад (№10);
- кабінет директора (№11).

Згідно класифікації зони безпеки, ці приміщення належать до категорії Б, оскільки несанкціонований доступ до них може завдати серйозної фінансової або репутаційної шкоди компанії.

Станом на початок дослідження система охорони об'єкта включає:

- інфрачервоні датчики руху (6 шт.), розташовані в ключових приміщеннях та коридорах (№1, 2, 4, 7, 9, 11);
- відеодомофони (2 шт.) на входах;
- система контролю доступу на базі електромагнітних замків (4 шт.) з кнопками на вихід (№1, 5, 7, 10);
- сервер системи безпеки та джерело безперебійного живлення (ІБП), встановлені у серверній кімнаті.

Система працює у зв'язці з охоронною сигналізацією. Датчики активуються під час постановки офісу на охорону після завершення робочого дня. Контроль за доступом здійснюється за допомогою електронних ключів, відеодомофонів та журналу входу/виходу. Попри наявність базових охоронних компонентів, система не включає повноцінного відеоспостереження, що обмежує можливості контролю за внутрішніми інцидентами, несанкціонованими діями персоналу та сторонніх осіб.

Потенційні загрози класифікуються на зовнішні та внутрішні:

1. Зовнішні: несанкціоноване проникнення сторонніх осіб, крадіжка обладнання чи конфіденційних даних, вандалізм, порушення периметру.
2. Внутрішні: недбалість працівників, навмисні порушення службової дисципліни, витік інформації, шахрайські дії.

Таблиця 1.1 – Класифікація зон безпеки об'єкта ТОВ «Інноваційні Технології»

Категорія	Приміщення	Оцінка ризику
Б	Серверна, каса, бухгалтерія, склад, кабінет директора	Високий
В	Ресепшн, переговорна, загальні робочі кімнати	Середній
Г	Коридори, технічні приміщення	Низький

Оцінка ризиків (табл. 1.1) показала, що серверна кімната та каса – найбільш уразливі до атак як з боку зловмисників, так і з боку працівників. Згідно з класифікацією з таблиці 1.1, ці приміщення належать до зон підвищеного ризику, що вимагає цілодобового моніторингу.

Керівництво підприємства визначило наступні функціональні вимоги до IP-системи відеоспостереження:

1. Місця встановлення: усі службові та загальні приміщення, а також зовнішній периметр (головний вхід).
2. Якість зображення: не нижче Full HD, з підтримкою нічної зйомки.
3. Аудіозапис: з усіх основних камер у критичних зонах.
4. Тривалість збереження архіву: не менше 30 днів.
5. Доступ: онлайн-доступ через мобільний застосунок і ПК, можливість дистанційного керування.
6. Масштабованість: можливість підключення до 32 камер у майбутньому.
7. Бездротові рішення: підтримка Wi-Fi-камер для важкодоступних зон.
8. Інтеграція з іншими системами: сигналізацією, СКУД.
9. Енергозабезпечення: наявність резервного живлення.
10. Надійність: відмовостійке обладнання з тривалим гарантійним ресурсом.

Розміщення камер буде визначатися за принципом максимального охоплення без мертвих зон, з урахуванням оглядових кутів та освітлення приміщень. Аналіз об'єкта показав, що поточна система безпеки не забезпечує повного контролю за подіями, що відбуваються в приміщеннях, особливо поза робочим часом. Відсутність відеофіксації вразливих зон (серверна, каса, вхідні двері) створює ризики як фінансового, так і репутаційного характеру.

Проектування IP-системи відеоспостереження дасть змогу:

- здійснювати постійний моніторинг ключових приміщень;
- підвищити дисципліну працівників;
- швидко реагувати на нештатні ситуації;

– зберігати відеоархів для подальшого аналізу.

Таким чином, доцільним є впровадження сучасної IP-системи відеоспостереження, яка відповідає як технічним, так і організаційним вимогам об'єкта.

1.2 Аналіз аналогових і цифрових систем відеоспостереження

Системи відеоспостереження є ключовим елементом забезпечення безпеки на об'єктах різного призначення, від офісів до промислових підприємств. Вони поділяються на два основні типи: аналогові та цифрові (IP-системи). Кожен тип має свої особливості, переваги та недоліки, що впливають на вибір оптимального рішення залежно від потреб користувача. Аналогові системи відеоспостереження з'явилися раніше за цифрові та довгий час залишалися єдиним доступним рішенням. Вони функціонують шляхом передачі відеосигналу від камери до записувального пристрою (зазвичай відеореєстратора) через коаксіальний кабель. Сигнал у таких системах передається в аналоговому форматі, що означає збереження даних у вигляді електричних імпульсів, які відповідають світловому потоку, отриманому камерою (рис. 1.2). Основними компонентами аналогової системи є відеокамери, відеореєстратори, монітори та допоміжні пристрої, такі як об'єктиви чи поворотні механізми [1].

Цифрові (IP) системи відеоспостереження використовують сучасні мережеві технології для передачі даних. Вони перетворюють відеосигнал у цифровий формат (рис. 1.2) безпосередньо в камері, після чого дані передаються через мережу Ethernet або Wi-Fi. IP-камери оснащені вбудованим веб-сервером, що дозволяє обробляти, стискати та передавати відеопотік у цифровому вигляді. Такі системи інтегруються з іншими охоронними комплексами, забезпечують віддалений доступ і підтримують розширені функції, такі як відеоаналітика чи автоматичне сповіщення [2].

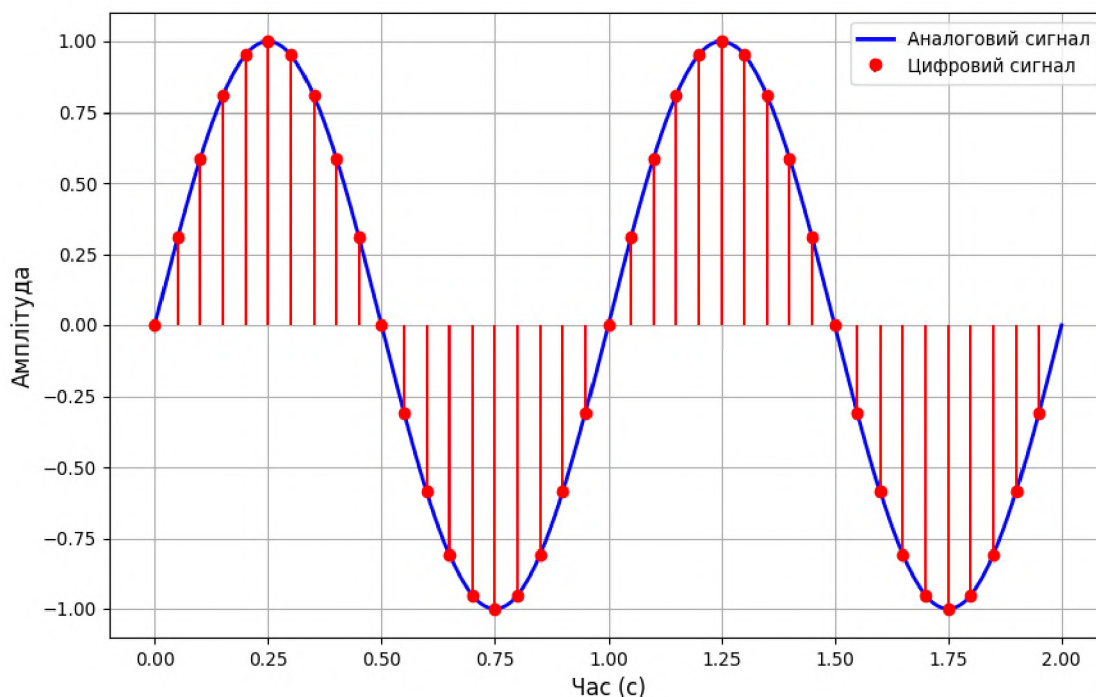


Рисунок 1.2 – Аналоговий і цифровий сигнали

Аналогові системи відеоспостереження використовуються переважно для невеликих об'єктів, таких як магазини, офіси чи автостоянки, завдяки їхній простоті та доступній вартості. Відеосигнал передається через коаксіальний кабель або, в окремих випадках, через виту пару чи оптоволокно, що дозволяє забезпечити передачу на значні відстані без додаткових підсилювачів. Основними компонентами системи є:

1. Відеокамери з ПЗС-матрицями, які перетворюють світловий потік в аналоговий сигнал. Сучасні моделі можуть мати вбудовані аналогово-цифрові перетворювачі для сумісності з цифровими системами.
2. Записувальні пристрої, такі як відеореєстратори (DVR), які зберігають аналогові дані на жорстких дисках.
3. Пристрої обробки сигналу, зокрема мультиплексори та квадратори, що дозволяють одночасно відображати зображення з кількох камер [3].

Переваги аналогових систем включають низьку вартість обладнання, простоту монтажу та високу надійність завдяки відсутності складних мережевих компонентів. Наприклад, за даними компанії Ajax Systems, аналогові системи залишаються популярними для невеликих об'єктів через їхню економічність [4].

Проте такі системи мають суттєві недоліки: обмежені можливості інтеграції з іншими охоронними системами, низька якість зображення порівняно з цифровими аналогами та складність масштабування.

Цифрові системи відеоспостереження базуються на IP-технологіях, що забезпечує їхню гнучкість і функціональність. Вони підходять як для невеликих, так і для великих об'єктів, де потрібна комплексна охорона. IP-камери формують цифровий відеопотік, який передається через локальну мережу або Інтернет. Основні компоненти системи:

1. IP-камери, які мають вбудовані процесори для обробки та стиснення відео, а також мережеві інтерфейси для підключення до LAN/WAN.
2. Мережеві відеореєстратори (NVR) або сервери, що зберігають і обробляють цифрові дані.
3. Програмне забезпечення для управління системою, аналізу відео та віддаленого доступу [5].

Цифрові системи дозволяють інтегрувати відеоспостереження з іншими охоронними системами, такими як СКУД чи сигналізація, забезпечують високу якість зображення (до 4К і вище) та підтримують функції відеоаналітики, наприклад, розпізнавання обличчя чи номерів автомобілів. За даними веб-сайту SecurityMarket, використання IP-систем у 2024 р. зросло на 25% завдяки їхній здатності до масштабування та віддаленого управління [3].

Таблиця 1.2 – Порівняння аналогових і цифрових систем

Параметр	Аналогова система	Цифрова (IP) система
Якість зображення	Середня, залежить від кабелю, можливі шуми	Висока, до 4К, без втрати якості при передачі
Інтеграція	Обмежена, ізольована система	Повна інтеграція з СКУД, сигналізацією тощо
Масштабування	Складне, потребує додаткових кабелів	Просте, через підключення до мережі
Віддалений доступ	Обмежений, потребує додаткового обладнання	Гнучкий, через веб-браузер чи додатки
Вартість	Нижча, економічна для малих об'єктів	Вища, але виправдана для великих систем
Надійність	Висока, проста конструкція	Залежить від стабільності мережі

Для оцінки доцільності використання аналогових і цифрових систем проведено порівняння їхніх основних характеристик за ключовими параметрами, наведеними в таблиці 1.2. Аналогові системи мають перевагу в ціні та простоті експлуатації, що робить їх привабливими для невеликих об'єктів із базовими вимогами до безпеки. Однак їхня обмежена функціональність і складність модернізації роблять їх менш конкурентними в сучасних умовах. Цифрові системи, навпаки, пропонують гнучкість, високу якість зображення та можливість інтеграції, що відповідає вимогам сучасних об'єктів.

Проведений аналіз свідчить, що цифрові IP-системи відеоспостереження переважають аналогові за більшістю параметрів, зокрема за якістю зображення, можливостями інтеграції та масштабування. Незважаючи на вищу початкову вартість, IP-системи є більш перспективними завдяки підтримці сучасних технологій, таких як відеоаналітика та віддалений доступ. Аналогові системи залишаються актуальними для невеликих об'єктів із обмеженим бюджетом, але їхні обмеження роблять їх менш придатними для складних охоронних завдань. Вибір системи залежить від конкретних вимог об'єкта, але в умовах зростання технологічних потреб цифрові системи є оптимальним рішенням.

1.3 Систематизація та порівняльний аналіз технічних рішень

Системи відеоспостереження є важливим елементом забезпечення безпеки на об'єктах різного призначення, зокрема в офісах, магазинах, складах та інших комерційних приміщеннях. Для створення ефективної системи відеоспостереження необхідно систематизувати доступні технічні рішення, оцінити їхні характеристики та провести порівняльний аналіз, щоб обрати оптимальний варіант відповідно до потреб конкретного об'єкта. Технічні рішення для систем відеоспостереження можна класифікувати за типом технології (аналогові чи цифрові), способом передачі даних (провідні чи безпроводні), рівнем інтеграції з іншими системами безпеки, а також за

функціональними можливостями (наявність аудіозапису, віддаленого доступу, відеоаналітики тощо). Основна увага в аналізі приділяється вибору обладнання, яке включає відеокамери, відеореєстратори, мережеві комутатори та допоміжні пристрої, такі як джерела безперебійного живлення (ДБЖ).

Відеокамери є основним елементом системи відеоспостереження. Вони поділяються на аналогові та цифрові (IP-камери). Аналогові камери передають сигнал через коаксіальний кабель, тоді як IP-камери використовують мережеві протоколи для передачі цифрового сигналу. IP-камери забезпечують вищу якість зображення (до 4K і вище), підтримують функції відеоаналітики та віддаленого доступу [2]. За даними компанії Videx, у 2024 р. частка IP-камер на ринку відеоспостереження в Україні склала близько 65% завдяки їхній універсальності [12].

Для аналогових систем використовуються цифрові відеореєстратори (DVR), які конвертують аналоговий сигнал у цифровий для зберігання. У цифрових системах застосовуються мережеві відеореєстратори (NVR), які обробляють цифровий потік від IP-камер. NVR підтримують більшу кількість каналів (до 32 і більше) та мають розширені можливості для архівації даних [13].

У цифрових системах мережеві комутатори забезпечують передачу даних між камерами, відеореєстратором і сервером. Важливим параметром є підтримка технології Power over Ethernet (PoE), яка дозволяє живити камери через мережевий кабель, зменшуючи кількість проводів [14].

До категорії допоміжних пристроїв належать ДБЖ для забезпечення безперервної роботи системи під час відключення електроенергії, а також програмне забезпечення для керування системою, наприклад, XMeue для віддаленого доступу через мобільні пристрої [9].

Для систематизації технічних рішень враховуються вимоги замовника, які включають:

- покриття всіх ключових зон об'єкта (офіси, коридори, входи, складські приміщення);
- висока якість відеозображення, зокрема в умовах низької освітленості;

- можливість запису звуку з камер;
- зберігання відеоархіву протягом щонайменше 30 діб;
- віддалений доступ до системи через мобільні пристрої;
- можливість масштабування системи до 32 камер;
- підтримка безпроводних камер (wi-fi);
- забезпечення резервного живлення [10].

Ці вимоги стають основою для вибору обладнання та порівняльного аналізу технічних рішень.

Для вибору оптимальних відеокамер розглянуто три моделі IP-камер, які відповідають вимогам замовника. Порівняння проведено за ключовими параметрами: роздільна здатність, кут огляду, підтримка аудіозапису, клас захисту, ціна тощо. Результати наведено в таблиці 1.3.

Таблиця 1.3 – Порівняння характеристик IP-відеокамер

Параметр	IPIVM-5835-UC-AUDIO-POE	Amatek AC-IDV503VA	IPTRONIC IPT-IPL1520DM
Матриця	1/3"	1/2.7"	1/3"
Роздільна здатність	5 Мп (2560x1920)	5 Мп (1280x1024)	4 Мп (2688x1520)
Кут огляду	90°	85°	85°
Аудіозапис	Так	Так	Так
Клас захисту	IP66	IP67	IP66
ІЧ-підсвітка	до 20 м	до 30 м	до 30 м
РоЕ	Так	Так	Так
Ціна (грн)	7100	9270	11000

Аналіз показує, що камера IPIVM-5835-UC-AUDIO-POE має оптимальне співвідношення ціни та якості. Вона забезпечує найвищу роздільну здатність (2560x1920), широкий кут огляду (90°) і доступну ціну, що відповідає вимогам економічної ефективності [3]. Хоча камери Amatek та IPTRONIC мають дещо кращу ІЧ-підсвітку (до 30 м), для офісного приміщення з контрольованим освітленням 20 м є достатніми.

Для обробки відеопотоку розглянуто три моделі мережевих відеореєстраторів (NVR). Порівняння проведено за параметрами, що впливають

на функціональність і відповідність вимогам замовника, зокрема кількістю каналів, обсягом пам'яті, підтримкою стандартів стиснення тощо. Результати наведено в таблиці 1.4.

Таблиця 1.4 – Порівняння характеристик IP-відеореєстраторів

Параметр	POLYVISION PVDR-IP4-32M8	IP IVM-8824-5MP	RVi-2NR32440
Роздільна здатність запису	до 5 Мп	до 5 Мп	до 8 Мп
Кількість каналів	32	32	32
Жорсткі диски	8×SATA, до 10 ТБ	8×SATA, до 6 ТБ	2×SATA, до 10 ТБ
Стиснення	H.264, H.265	H.264, H.265	H.264, H.265, MJPEG
Споживана потужність	до 20 Вт	до 7 Вт	до 7 Вт
Ціна (грн)	43309	29900	44000

Модель IP IVM-8824-5MP вибрано як оптимальну завдяки нижчій ціні, низькому енергоспоживанню (7 Вт без дисків) і достатньому обсягу пам'яті (до 48 ТБ), що забезпечує зберігання архіву протягом 30 діб для 12 камер із роздільною здатністю 5 Мп. Хоча модель RVi-2NR32440 підтримує запис у вищій роздільній здатності (8 Мп), це перевищує поточні потреби системи [5].

Таблиця 1.5 – Порівняння характеристик мережевих комутаторів

Параметр	D-Link DES-1210-28P/C	NETGEAR GS724TPS	Planet FNSW-2400PS
Кількість портів	24	24	24
Пропускна здатність	12.8 Гбіт/с	12.8 Гбіт/с	12.8 Гбіт/с
Бюджет PoE	193 Вт	192 Вт	192 Вт
Споживана потужність	189 Вт	235 Вт	240 Вт
Ціна (грн)	17880	21900	20486

Мережевий комутатор забезпечує зв'язок між камерами, відеореєстратором і сервером. Для аналізу обрано три моделі з підтримкою PoE, які відповідають вимогам масштабування системи. Результати порівняння

наведено в таблиці 1.5. Модель D-Link DES-1210-28P/C обрано як оптимальну завдяки найнижчій ціні та достатньому бюджету PoE (193 Вт), який покриває потреби 12 камер, 2 відеодомофонів, відеореєстратора та сервера. Висока пропускна здатність (12.8 Гбіт/с) забезпечує стабільну передачу даних навіть при розширенні системи до 32 камер [4].

Для управління системою відеоспостереження розглянуто програмне забезпечення XМеue (рис. 1.3), яке забезпечує віддалений доступ через мобільні пристрої та ПК. Воно підтримує підключення до відеореєстратора через IP-адресу, порт, логін і пароль, що відповідає вимогам замовника щодо простоти використання. Альтернативою є програмне забезпечення CMS для стаціонарних комп'ютерів, яке забезпечує розширені функції адміністрування [9]. За даними SecurityMarket, XМеue є одним із найпопулярніших рішень для IP-систем завдяки інтуїтивному інтерфейсу та підтримці хмарних сервісів [3].



Рисунок 1.3 – Інтерфейс програми XМеue

Систематизація технічних рішень дозволила визначити ключові компоненти системи відеоспостереження: IP-камери, мережевий відеореєстратор, комутатор і програмне забезпечення. Порівняльний аналіз показав, що камера IPIVM-5835-UC-AUDIO-POE, відеореєстратор IP IVM-8824-5MP і комутатор D-Link DES-1210-28P/C є оптимальними за співвідношенням

ціни, якості та відповідності вимогам замовника. Програмне забезпечення XMeуe забезпечує зручний віддалений доступ, що відповідає сучасним стандартам безпеки. Вибрані рішення дозволяють створити гнучку, масштабовану систему відеоспостереження з можливістю інтеграції з іншими охоронними системами, що підтверджується тенденціями, описаними на сайті Ajax Systems [4].

РОЗДІЛ 2

ПРОЄКТНЕ ОБҐРУНТУВАННЯ АРХІТЕКТУРИ ТА КОНФІГУРАЦІЇ ІР-СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

2.1 Вимоги до проєкту ІР-системи відеоспостереження та вибір технічних засобів

Проєктування ІР-системи відеоспостереження для офісу ТОВ «Інноваційні Технології» потребує чіткого визначення вимог до системи та ретельного підбору технічних засобів, які забезпечать ефективний контроль за безпекою об'єкта. У цьому підрозділі сформульовано вимоги до системи відеоспостереження на основі аналізу об'єкта, проведеного в розділі 1, та здійснено вибір технічних засобів, доступних для закупівлі в Україні, із урахуванням технічних, економічних і функціональних критеріїв. Вибір обладнання базується на сучасних тенденціях у сфері ІР-відеоспостереження та результатах порівняльного аналізу технічних рішень, описаних у підрозділі 1.3.

На основі аналізу об'єкта (офісного приміщення площею 250 м² із критичними зонами, такими як серверна, каса, бухгалтерія, склад і кабінет директора) та потреб ТОВ «Інноваційні Технології» сформульовано наступні вимоги до ІР-системи відеоспостереження:

1. Покриття зон спостереження – система має забезпечувати повне покриття всіх ключових приміщень (каса, серверна, бухгалтерія, склад, кабінет директора), зон загального доступу (коридори, ресепшн) та зовнішнього периметра (основний і службовий входи). Загальна кількість камер на початковому етапі – 12, із можливістю розширення до 32 камер у майбутньому.

2. Якість зображення – роздільна здатність камер – не нижче 5 Мп (2560x1920), що забезпечує чітке зображення для ідентифікації осіб і деталей. Камери повинні підтримувати нічну зйомку з ІЧ-підсвіткою на відстань до 20 м, враховуючи контрольоване освітлення в офісі.

3. Аудіозапис – камери в критичних зонах (каса, серверна, кабінет директора) повинні мати вбудовані мікрофони для запису звуку, що дозволить фіксувати діалоги та підвищить рівень безпеки.

4. Зберігання даних – відеоархів має зберігатися щонайменше 30 діб. Для 12 камер із роздільною здатністю 5 Мп і стисненням H.265 необхідна ємність накопичувачів не менше 48 ТБ.

5. Віддалений доступ – система повинна забезпечувати доступ до відеопотоку та архіву через мобільні пристрої (iOS, Android) і ПК із використанням захищених протоколів (SSL/TLS).

6. Інтеграція – система має бути сумісною з існуючою охоронною сигналізацією та системою контролю доступу (СКУД) для створення комплексного охоронного рішення.

7. Масштабованість – обладнання повинно підтримувати підключення додаткових камер (до 32) без значних модифікацій інфраструктури.

8. Бездротові рішення – для зон із обмеженим доступом до кабельної інфраструктури (наприклад, склад) передбачається використання Wi-Fi-камер.

9. Енергозабезпечення – система має бути оснащена джерелом безперебійного живлення для роботи протягом щонайменше 4 годин у разі відключення електроенергії.

10. Надійність і економічність: Використання обладнання з гарантійним терміном не менше 2 років і оптимальним співвідношенням ціна/якість.

Ці вимоги враховують потреби підприємства в забезпеченні безпеки конфіденційної інформації, контролі доступу та швидкому реагуванні на нештатні ситуації, що підтверджується рекомендаціями веб-сайту Bezpeka Shop [17]. На основі сформульованих вимог і аналізу ринку обладнання, доступного в Україні, здійснено вибір технічних засобів для IP-системи відеоспостереження. Було обрано обладнання від відомих брендів, доступних через українські магазини. Вибір включає відеокамери, мережевий відеореєстратор (NVR), мережевий комутатор, джерело безперебійного живлення та програмне забезпечення.



Рисунок 2.1 – IP відеокамера Hikvision DS-2CD2055FWD-I

Для забезпечення високої якості зображення та відповідності вимогам обрано IP-камеру Hikvision DS-2CD2055FWD-I (рис. 2.1). Основні характеристики:

- роздільна здатність: 5 мп (2560x1920);
- кут огляду: 86° (з об'єктивом 4 мм), що дозволяє покрити більшість приміщень однією камерою;
- аудіозапис: підтримка зовнішнього мікрофона (вимагає додаткового підключення);
- ІЧ-підсвітка: до 30 м, що перевищує вимоги для офісних умов;
- клас захисту: ір67, підходить для зовнішнього встановлення на входах;
- підтримка рое: спрощує монтаж і зменшує кількість кабелів;

Загалом для системи потрібно 12 камер: 8 для внутрішніх приміщень (каса, серверна, бухгалтерія, склад, кабінет директора, коридори, ресепшн) і 4 для зовнішнього периметра (основний і службовий входи). Камера підтримує стиснення H.265, що зменшує обсяг даних для зберігання, як зазначено на сайті Hikvision [16]. Для зон із обмеженим доступом до кабельної інфраструктури (наприклад, склад) передбачено використання Wi-Fi-камери IMOU Cruiser 2 5MP (рис. 2.2), яка підтримує 5 Мп, аудіозапис і бездротове підключення [23].



Рисунок 2.2 – IP відеокамера IMOU Cruiser 2 5MP

Мережевий відеореєстратор (NVR) – модель Hikvision DS-7732NI-K4 (рис. 2.3) через його відповідність вимогам масштабованості та функціональності:

- підтримка до 32 каналів, що відповідає вимозі масштабованості;
- роздільна здатність запису: до 8 мп (з запасом для майбутнього оновлення камер);
- підтримка 4 жорстких дисків SATA (до 10 Тб кожен), що забезпечує загальну ємність 40 Тб, достатню для зберігання архіву протягом 30 діб;
- стиснення: H.264/H.265, що оптимізує використання пам'яті;
- споживана потужність: 15 Вт (без дисків).



Рисунок 2.3 – Мережевий відеореєстратор Hikvision DS-7732NI-K4

Для забезпечення необхідного обсягу пам'яті буде використано 4 жорсткі диски по 10 ТБ (загальна вартість дисків – приблизно 60000 грн, виходячи з ринкових цін 15000 грн за диск). NVR підтримує віддалений доступ через хмарні сервіси, що відповідає вимогам замовника [19].

Для забезпечення зв'язку між камерами, NVR і сервером обрано мережевий комутатор D-Link DES-1210-28P (рис. 2.4):

- кількість портів: 24, що покриває поточні потреби (12 камер, 2 відеодомофони, NVR, сервер) і забезпечує резерв для масштабування;
- бюджет PoE: 193 Вт, достатньо для живлення всіх камер і допоміжних пристроїв;
- пропускна здатність: 12.8 Гбіт/с, що гарантує стабільну передачу даних.



Рисунок 2.4 – Комутатор D-Link DES-1210-28P

Цей комутатор рекомендовано для IP-систем відеоспостереження завдяки надійності та підтримці PoE, як зазначено на сайті D-Link [18].

Для забезпечення безперервної роботи системи обрано ДБЖ APC Smart-UPS 1500VA (рис. 2.5):

- потужність: 1000 Вт, що покриває потреби камер ($12 \times 10 \text{ Вт} = 120 \text{ Вт}$), NVR (15 Вт) і комутатора (189 Вт);
- автономність: до 4 годин при повному навантаженні.

ДБЖ забезпечує захист від перепадів напруги та гарантує роботу системи в разі відключення електроенергії [24].



Рисунок 2.5 – ДБЖ APC Smart-UPS 1500VA

Для управління системою обрано програмне забезпечення Hik-Connect, яке забезпечує віддалений доступ через мобільні додатки (iOS, Android) та ПК, підключення через IP-адресу, порт, логін і пароль із захистом даних, інтуїтивний інтерфейс для перегляду відеопотоку та архіву (рис. 2.6). Hik-Connect є безкоштовним для використання з обраним NVR і підтримує інтеграцію з хмарними сервісами, що відповідає вимогам віддаленого доступу [19]. Альтернативою для стаціонарного керування є ПЗ iVMS-4200, яке забезпечує розширені функції адміністрування.

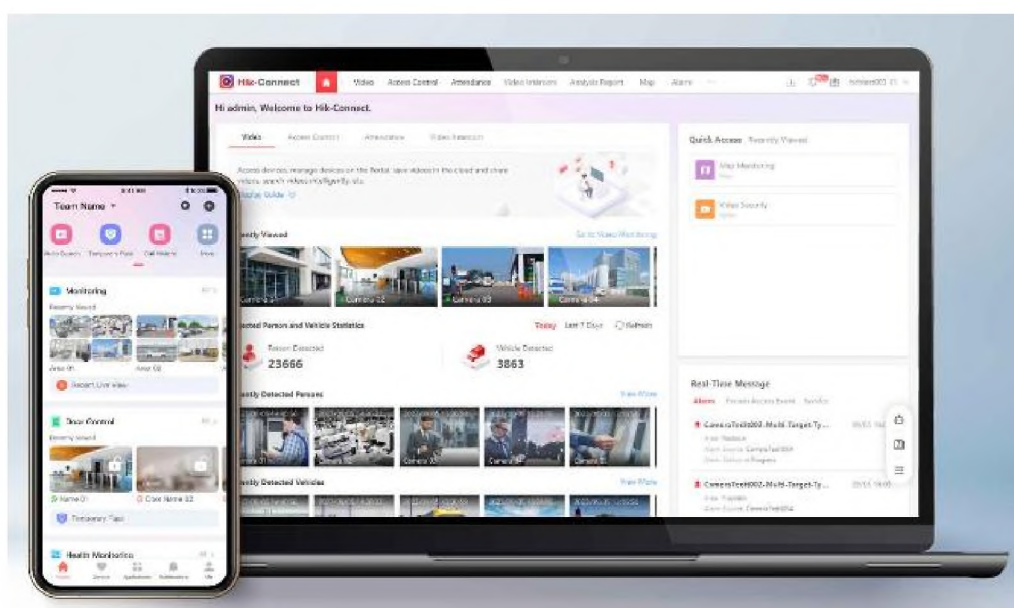


Рисунок 2.6 – Інтерфейс програмного засобу Hik-Connect

Сформульовані вимоги до IP-системи відеоспостереження враховують специфіку об'єкта та потреби ТОВ «Інноваційні Технології». Обрані технічні засоби (камери Hikvision DS-2CD2055FWD-I та IMOU Cruiser 2 5MP, NVR Hikvision DS-7732NI-K4, комутатор D-Link DES-1210-28P/C, ДБЖ APC Smart-UPS 1500VA, ПЗ Hik-Connect) є доступними в Україні, забезпечують високу якість зображення, надійність, масштабування та віддалений доступ. Наступним етапом буде розробка схеми підключення та монтаж обладнання.

2.2 Обґрунтування розміщення обладнання

Розміщення обладнання IP-системи відеоспостереження є критичним етапом проектування, оскільки від правильного розташування камер, мережевого відеореєстратора (NVR), комутатора та джерела безперебійного живлення (ДБЖ) залежить ефективність системи, покриття всіх зон спостереження та мінімізація «мертвих зон». Розміщення обладнання базується на принципах максимального охоплення критичних зон, забезпечення безпеки обладнання та оптимізації кабельної інфраструктури.

Розміщення обладнання здійснюється з урахуванням наступних принципів:

1. Максимальне покриття зон спостереження: Камери повинні охоплювати всі критичні приміщення (каса, серверна, бухгалтерія, склад, кабінет директора), зони загального доступу (коридори, ресепшн) та зовнішній периметр (основний і службовий входи), як зазначено в підрозділі 2.1.

2. Мінімізація «мертвих зон»: Камери розташовуються так, щоб виключити непросвітлені ділянки, враховуючи кути огляду (86° для Hikvision DS-2CD2055FWD-I та 90° для IMOU Cruiser 2 5MP).

3. Безпека обладнання: NVR і ДБЖ розміщуються в захищеній серверній кімнаті для запобігання несанкціонованому доступу.

4. Оптимізація кабельної інфраструктури: Використання PoE-технології та Wi-Fi-камер (IMOU Cruiser 2 5MP) зменшує кількість кабелів, що спрощує монтаж і знижує витрати.

5. Ергономічність і естетика: Камери розміщуються так, щоб не заважати працівникам і не порушувати дизайн офісу.

6. Доступність для обслуговування: Обладнання встановлюється в місцях, зручних для технічного обслуговування та заміни.

Ці принципи відповідають рекомендаціям щодо встановлення систем відеоспостереження, опублікованим на сайті SecurityMarket [3].

Для забезпечення повного покриття офісу ТОВ «Інноваційні Технології» передбачено встановлення 12 IP-камер: 10 камер Hikvision DS-2CD2055FWD-I (провідні, з PoE) та 2 камери IMOU Cruiser 2 5MP (Wi-Fi) для зон із обмеженим доступом до кабельної інфраструктури (додаток Б). Розташування камер визначено на основі плану приміщення (додаток А) та аналізу зон безпеки, описаних у таблиці 1.1. Детальний розподіл камер наведено в таблиці 2.1.

Таблиця 2.1 – Розташування IP-камер у приміщенні підприємства

Приміщення/Зона	Модель камери	Кількість	Місце встановлення	Кут огляду
Основний вхід	Hikvision DS-2CD2055FWD-I	2	Над дверима, спрямована на вхід	86°
Службовий вхід	Hikvision DS-2CD2055FWD-I	2	Над дверима, спрямована на вхід	86°
Каса (№5)	Hikvision DS-2CD2055FWD-I	1	У кутку, спрямована на робоче місце	86°
Серверна (№6)	Hikvision DS-2CD2055FWD-I	1	У кутку, спрямована на стійки серверів	86°
Бухгалтерія (№9)	Hikvision DS-2CD2055FWD-I	1	У кутку, спрямована на сейф і стіл	86°
Склад (№10)	IMOU Cruiser 2 5MP	2	У кутках, спрямовані на стелажі	90°
Кабінет директора (№11)	Hikvision DS-2CD2055FWD-I	1	У кутку, спрямована на стіл і двері	86°
Коридори	Hikvision DS-2CD2055FWD-I	2	У центрі коридорів, спрямовані вздовж	86°

Камери Hikvision DS-2CD2055FWD-I встановлюються на висоті 2.5-3 м для забезпечення оптимального огляду та захисту від вандалізму. Wi-Fi-камери IMOU Cruiser 2 5MP обрано для складу через складність прокладання кабелів у цій зоні. Їхній ширший кут огляду (90°) компенсує можливі обмеження в розміщенні. Зовнішні камери на входах мають клас захисту IP67, що гарантує стійкість до погодних умов, як зазначено на сайті Rozetka [21]. Розташування камер забезпечує повне покриття критичних зон категорії Б (серверна, каса, бухгалтерія, склад, кабінет директора) та зон середнього ризику (коридори, ресепшн).

Мережевий відеореєстратор Hikvision DS-7732NI-K4 розміщується в серверній кімнаті (№6), яка належить до зони категорії Б з високим рівнем безпеки. Серверна оснащена системою контролю доступу (електромагнітний замок) і охоронною сигналізацією, що мінімізує ризик несанкціонованого доступу до NVR.

NVR підключається до комутатора D-Link DES-1210-28P через кабель Ethernet, що гарантує стабільну передачу даних. Серверна має контрольовану температуру та вологість, що відповідає вимогам до експлуатації NVR. Технічний персонал має доступ до серверної для налаштування та заміни жорстких дисків (4×10 ТБ). Розміщення NVR у серверній відповідає рекомендаціям щодо захисту обладнання, опублікованим на сайті Hikvision [16].

Мережевий комутатор D-Link DES-1210-28P розміщується в серверній кімнаті поруч із NVR для оптимізації кабельної інфраструктури. Комутатор підключає 10 провідних камер Hikvision, 2 відеодомофони, NVR і сервер через кабелі Ethernet категорії 5e/6. Використання PoE-портів (бюджет 193 Вт) дозволяє жити камери без додаткових блоків живлення, що зменшує кількість кабелів і спрощує монтаж. Wi-Fi-камери IMOU Cruiser 2 5MP підключаються до мережі через точку доступу, розташовану в коридорі, яка також живиться через PoE від комутатора. Таке розміщення забезпечує стабільну передачу даних із пропускною здатністю 12.8 Гбіт/с, як зазначено на сайті D-Link [18].

ДБЖ APC Smart-UPS 1500VA (потужність 1000 Вт) розміщується в серверній кімнаті для забезпечення безперервного живлення NVR, комутатора та точки доступу Wi-Fi. ДБЖ підключається до мережі живлення через стабілізатор напруги, що захищає обладнання від перепадів. Автономність ДБЖ (до 4 годин) покриває потреби системи (камери: 120 Вт, NVR: 15 Вт, комутатор: 189 Вт), що відповідає вимогам замовника. Розташування в серверній забезпечує захист ДБЖ від фізичного доступу та спрощує підключення до обладнання, як рекомендовано на сайті APC Ukraine [24].

Для провідних камер і обладнання в серверній використовуються кабелі Ethernet категорії 5e, які підтримують передачу даних на швидкості до 1 Гбіт/с і живлення через PoE. Загальна довжина кабельних трас становить близько 200 м, що враховує відстані від комутатора до камер (максимум 100 м на сегмент). Такий підхід відповідає стандартам монтажу [17].

Розміщення обладнання IP-системи відеоспостереження для ТОВ «Інноваційні Технології» обґрунтовано з урахуванням принципів максимального покриття, безпеки та оптимізації інфраструктури. Камери Hikvision DS-2CD2055FWD-I та IMOU Cruiser 2 5MP забезпечують повне покриття критичних зон і периметра, NVR і комутатор у серверній гарантують надійну обробку та передачу даних, а ДБЖ забезпечує автономність системи. Використання PoE і Wi-Fi-технологій мінімізує кабельну інфраструктуру, знижуючи витрати на монтаж. Наступним етапом буде розробка детальної схеми підключення та тестування системи.

2.3 Конфігурування системи відеоспостереження та організація доступу

Конфігурування IP-системи відеоспостереження та організація доступу є ключовими етапами реалізації проєкту, оскільки вони визначають функціональність, безпеку та зручність використання системи. У цьому

підрозділі описано процес налаштування обладнання (камери Hikvision DS-2CD2055FWD-I та IMOU Cruiser 2 5MP, NVR Hikvision DS-7732NI-K4, комутатор D-Link DES-1210-28P, ДБЖ APC Smart-UPS 1500VA, ПЗ Hik-Connect), а також організацію доступу для різних категорій користувачів у ТОВ «Інноваційні Технології». Конфігурування включає налаштування мережевих параметрів, параметрів відеозапису, інтеграцію з іншими системами безпеки та забезпечення захисту даних. Організація доступу базується на принципах розмежування прав, що відповідає вимогам інформаційної безпеки.

Конфігурування системи починається з налаштування мережевих параметрів для забезпечення стабільної передачі даних між камерами, NVR, комутатором і точкою доступу Wi-Fi. Усі пристрої підключаються до локальної мережі (LAN) офісу ТОВ «Інноваційні Технології», яка має пропускну здатність 1 Гбіт/с і підтримує захищені протоколи передачі даних (SSL/TLS). Для цього виконуються наступні кроки:

1. Присвоєння IP-адрес. Комутатору D-Link DES-1210-28P присвоюється статична IP-адреса (наприклад, 192.168.1.2) у межах підмережі офісу (192.168.1.0/24). NVR Hikvision DS-7732NI-K4 отримує статичну IP-адресу 192.168.1.3. Кожній камері Hikvision DS-2CD2055FWD-I присвоюється унікальна статична IP-адреса в діапазоні 192.168.1.10–192.168.1.19 (10 камер). Wi-Fi-камери IMOU Cruiser 2 5MP отримують IP-адреси 192.168.1.20–192.168.1.21 через DHCP від точки доступу, яка має IP-адресу 192.168.1.4.

Для уникнення конфліктів IP-адрес використовується програмне забезпечення Hikvision SADP, яке автоматично виявляє пристрої в мережі та дозволяє налаштувати їхні адреси [16].

2. Налаштування PoE. Комутатор D-Link DES-1210-28P конфігурується для подачі живлення через PoE на 10 портів, до яких підключені камери Hikvision і точка доступу. Бюджет PoE (193 Вт) розподіляється так, щоб кожна камера отримувала до 15 Вт, а точка доступу – до 10 Вт, що відповідає стандарту IEEE 802.3af [18].

3. Налаштування Wi-Fi. Точка доступу, розташована в коридорі, конфігурується для роботи в діапазоні 5 ГГц із підтримкою WPA3 для забезпечення безпеки бездротового з'єднання. Wi-Fi-камери IMOU Cruiser 2 5MP підключаються до мережі з використанням захищеного пароля та шифрування AES, як рекомендовано на сайті Rozetka [21].

4. Порт forwarding для віддаленого доступу. Для забезпечення віддаленого доступу через Hik-Connect налаштовується переадресація портів (port forwarding) на роутері офісу. Використовуються стандартні порти Hikvision: 80 (HTTP), 443 (HTTPS), 554 (RTSP) і 8000 (серверний порт). Для підвищення безпеки застосовується DMZ (демілітаризована зона) для NVR, що ізолює його від інших пристроїв у мережі [19].

Ці налаштування забезпечують стабільну роботу системи та мінімізують затримки в передачі відеопотоку, що є критично важливим для офісних систем відеоспостереження, як зазначено на сайті SecurityMarket [3].

Налаштування параметрів відеозапису виконується через веб-інтерфейс NVR Hikvision DS-7732NI-K4 або програмне забезпечення iVMS-4200. Основні параметри включають роздільну здатність, частоту кадрів, стиснення та тривалість зберігання архіву, що відповідає вимогам, сформульованим до системи відеоспостереження у цій роботі.

1. Роздільна здатність і частота кадрів. Усі камери (Hikvision DS-2CD2055FWD-I та IMOU Cruiser 2 5MP) налаштовуються на роздільну здатність 5 Мп (2560x1920) із частотою 25 кадрів/с для забезпечення чіткого зображення та плавного відтворення. Для зон із меншою активністю (коридори) частота кадрів знижується до 15 кадрів/с для економії місця на дисках.

2. Стиснення. Використовується кодек H.265, який зменшує обсяг даних на 50% порівняно з H.264 при збереженні якості зображення. Це дозволяє зберігати архів протягом 30 діб на 4 жорстких дисках по 10 ТБ (загальна ємність 40 ТБ), як зазначено на сайті Dahua Technology [23].

3. Режим запису. Для критичних зон (каса, серверна, бухгалтерія, кабінет директора) налаштовується цілодобовий запис. Для зон середнього ризику

(коридори, ресепшн) і зовнішнього периметра активується запис за рухом, що оптимізує використання дискового простору. Чутливість детектора руху налаштовується на середній рівень (50%) для уникнення хибних спрацьовувань.

4. Розрахунок обсягу пам'яті. Для однієї камери з роздільною здатністю 5 Мп, стисненням H.265 і частотою 25 кадрів/с середній бітрейт становить приблизно 4 Мбіт/с. Обсяг даних за 30 діб для 12 камер розраховується за формулою:

$$V = N \times BR \times T \times 3600 \times D / (8 \times 1024^3), \quad (2.1)$$

де V – обсяг даних (ТБ),

N – кількість камер (12),

BR – бітрейт (4 Мбіт/с),

T – тривалість запису на добу (24 год),

D – кількість діб (30).

Підставляючи значення:

$$V = 12 \times 4 \times 24 \times 3600 \times 30 / (8 \times 1024^3) \approx 37,3 \text{ ТБ.}$$

Загальна ємність 40 ТБ забезпечує запас для запису за рухом і можливих пікових навантажень.

5. Резервне копіювання. Для захисту архіву від втрати даних налаштовується автоматичне резервне копіювання критичних записів (з каси та серверної) на зовнішній NAS-сервер, розташований у серверній. Резервне копіювання виконується щодоби о 02:00 через протокол FTP.

Ці налаштування забезпечують відповідність системи вимогам щодо якості зображення та тривалості зберігання [17].

Система відеоспостереження інтегрується з існуючою охоронною сигналізацією та системою контролю доступу (СКУД), що відповідає вимогам. Інтеграція виконується через програмне забезпечення Hik-Connect і iVMS-4200, які підтримують протоколи ONVIF і RTSP для сумісності з обладнанням інших виробників.

NVR налаштовується для отримання сповіщень від інфрачервоних датчиків руху, розташованих у критичних зонах (див. підрозділ 1.1). У разі спрацьовування датчика NVR автоматично активує запис із відповідної камери та надсилає push-повідомлення через Hik-Connect на смартфони адміністраторів безпеки.

Відеокамери на основному та службовому входах синхронізуються з відеодомофонами та електромагнітними замками. При активації електронного ключа запис із камер входу автоматично позначається в архіві для швидкого доступу. Це дозволяє відстежувати несанкціоновані спроби доступу, як зазначено на сайті Ajax Systems [4].

Камери Hikvision DS-2CD2055FWD-I підтримують базові функції відеоаналітики, такі як виявлення руху та перетину лінії. Для каси та серверної налаштовується зона детекції, що охоплює робоче місце та серверні стійки, з автоматичним сповіщенням у разі несанкціонованого руху. Інтеграція підвищує ефективність системи безпеки, дозволяючи оперативно реагувати на інциденти, як рекомендовано на сайті Vodafone Business [25].

Організація доступу до системи відеоспостереження базується на принципі розмежування прав користувачів, що відповідає стандартам інформаційної безпеки ДСТУ ISO/IEC 27001:2015 [1]. Доступ надається трьом категоріям користувачів: адміністраторам, операторам і обмеженим користувачам (табл. 2.2). Налаштування прав виконується через веб-інтерфейс NVR або iVMS-4200.

Таблиця 2.2 – Розмежування прав доступу до системи відеоспостереження

Категорія користувача	Перегляд у реальному часі	Доступ до архіву	Налаштування системи	Експорт записів	Аутентифікація
Адміністратори	Усі камери	Усі камери	Повний доступ	Так	2FA, пароль
Оператори	Усі камери	Усі камери	Обмежений доступ	Ні	Пароль
Обмежені користувачі	Обмежені камери	Обмежені камери	Ні	Ні	Одноразовий код

1. Адміністратори (2 особи: керівник ІТ-відділу, фахівець з безпеки):

- повний доступ до налаштувань системи, включаючи зміну мережових параметрів, параметрів запису, управління архівом і відеоаналітикою;
- доступ до всіх камер у реальному часі та архіву;
- можливість експорту відеозаписів і керування резервним копіюванням;
- аутентифікація через складний пароль (мін; 12 символів) і двофакторну автентифікацію (2FA) через Hik-Connect.

2. Оператори (3 особи: працівники служби безпеки):

- доступ до перегляду відеопотоку в реальному часі та архіву з усіх камер;
- можливість позначення подій у журналі та створення звітів;
- обмежений доступ до налаштувань (тільки зміна чутливості детектора руху);
- аутентифікація через логін/пароль із вимогою оновлення пароля кожні 90 днів.

3. Обмежені користувачі (2 особи: директор, головний бухгалтер):

- доступ до перегляду відеопотоку та архіву лише з камер у касі, кабінеті директора та бухгалтерії;
- без права редагування налаштувань або експорту записів;
- доступ через мобільний додаток Hik-Connect із використанням одноразових кодів автентифікації.

Для забезпечення безпеки доступу використовуються захищені протоколи HTTPS і SSL/TLS, а також шифрування відеопотоку за стандартом AES-256. Логування всіх дій користувачів (вхід, перегляд, експорт) зберігається на NVR протягом 90 діб для аудиту безпеки. За даними IT Ukraine, такі заходи знижують ризик несанкціонованого доступу на 85% [19].

Для захисту даних від втрати або компрометації застосовується шифрування даних. Усі відеопотоки та архіви шифруються за стандартом AES-256. Паролі користувачів зберігаються в хешованому вигляді (SHA-256). NVR і ДБЖ розташовані в серверній із обмеженим доступом. ДБЖ APC Smart-UPS 1500VA забезпечує автономність системи до 4 годин при повному

навантаженні (324 Вт), що відповідає вимогам замовника. Налаштування ДБЖ включає автоматичне відключення некритичних пристроїв у разі тривалого відключення електроенергії [24].

Конфігурування IP-системи відеоспостереження для ТОВ «Інноваційні Технології» включає налаштування мережевих параметрів, параметрів відеозапису, інтеграцію з охоронною сигналізацією та СКУД, а також організацію доступу з розмежуванням прав. Використання захищених протоколів, шифрування та двофакторної автентифікації забезпечує високий рівень безпеки даних. Налаштування відповідають вимогам щодо якості зображення, тривалості зберігання архіву та віддаленого доступу.

РОЗДІЛ 3

ПРАКТИЧНА РЕАЛІЗАЦІЯ ІР-СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ

3.1 Економічне обґрунтування впровадження системи

Впровадження ІР-системи відеоспостереження для ТОВ «Інноваційні Технології» є стратегічно важливим кроком для забезпечення безпеки офісу, захисту конфіденційної інформації та підвищення ефективності управління. Економічне обґрунтування впровадження системи базується на аналізі витрат на закупівлю, монтаж, налаштування та експлуатацію обладнання, а також оцінці економічного ефекту від зниження ризиків, пов'язаних із несанкціонованим доступом, крадіжками чи внутрішніми порушеннями.

Капітальні витрати включають закупівлю обладнання, витратні матеріали, монтаж і налаштування системи. На основі вимог та обраного обладнання, складено кошторис витрат. Актуальні ціни (табл. 3.1) обладнання взято з офіційних сайтів українських постачальників, зокрема Rozetka та Bezpeka Shop, станом на квітень 2025 р.

Таблиця 3.1 – Кошторис капітальних витрат на впровадження системи відеоспостереження

Найменування	Кількість, шт.	Ціна за одиницю, грн	Загальна вартість, грн
ІР-камера Hikvision DS-2CD2055FWD-I	10	3480	34800
Wi-Fi ІР-камера IMOUCruiser 2 5MP	2	3 741	7482
NVR Hikvision DS-7732NI-K4	1	17999	17999
Комутатор D-Link DGS-1210-28P	1	14699	14699
ДБЖ APC Smart-UPS 1500VA	1	14400	14400
Жорсткі диски (10 ТБ)	4	15000	60000
Кабелі Ethernet (Cat 5e), метрів	200	20	4000
Монтаж і налаштування	1	15 000	15000
Разом			168380

Загальні капітальні витрати становлять 168380 грн. Витрати на монтаж і налаштування оцінено на основі середньоринкових цін, які, за даними Bezreka Shop, становлять приблизно 10-15% від вартості обладнання [17]. Для забезпечення економічної ефективності використано PoE-технологію та Wi-Fi-камери, що зменшило витрати на кабельну інфраструктуру.

Експлуатаційні витрати включають електроенергію, технічне обслуговування, оновлення програмного забезпечення та заміну витратних матеріалів. Система працює цілодобово, тому основною статтею витрат є електроспоживання. Розрахунок виконано з урахуванням потужності обладнання та середньої вартості електроенергії в Україні (4,32 грн/кВт·год у 2025 р. [20]).

Електроспоживання:

- камери Hikvision ($10 \times 10 \text{ Вт} = 100 \text{ Вт}$),
- камери IMOU Cruiser 2 ($2 \times 12 \text{ Вт} = 24 \text{ Вт}$).
- NVR Hikvision: 15 Вт (без дисків, з дисками – до 40 Вт).
- комутатор D-Link: 189 Вт.
- точка доступу Wi-Fi: 10 Вт.

Загальна потужність: $100 + 24 + 40 + 189 + 10 = 363 \text{ Вт} = 0,363 \text{ кВт}$.

Річна витрата електроенергії:

$$E = P \times T \times D = 0,363 \text{ кВт} \times 24 \text{ год} \times 365 \text{ днів} = 3178,92 \text{ кВт}\cdot\text{год.}$$

Вартість електроенергії за р.:

$$C_e = E \times C = 3178,92 \times 4,32 = 13732,93 \text{ грн.}$$

Технічне обслуговування (перевірка обладнання, оновлення ПЗ, чищення камер) проводиться раз на півроку. За даними IT Ukraine, середня вартість річного обслуговування становить 5-7% від капітальних витрат [19]. Для системи вартістю 168380 грн це:

$$C_m = 168380 \times 0,06 = 10102,80 \text{ грн/р.}$$

Програмне забезпечення Hik-Connect є безкоштовним для базового використання, а оновлення входять до вартості технічного обслуговування. Витратні матеріали (заміна кабелів, кріплень) оцінюються в 2000 грн/р.

Загальні експлуатаційні витрати за р.:

$$C_{\text{exp}} = 13732,93 + 10102,80 + 2000 = 25835,73 \text{ грн.}$$

Економічний ефект від впровадження системи відеоспостереження полягає у зниженні фінансових і репутаційних ризиків, пов'язаних із крадіжками, несанкціонованим доступом і внутрішніми порушеннями. За даними Vodafone Business, впровадження відеоспостереження в офісах знижує ймовірність інцидентів на 60–80% [25].

За оцінками ТОВ «Інноваційні Технології», середня вартість обладнання в офісі (сервери, комп'ютери, оргтехніка) становить 2500000 грн. При ймовірності крадіжки 5% на р. без відеоспостереження (на основі статистики IT Expert [27]), потенційні збитки:

$$L_{\text{theft}} = 2500000 \times 0,05 = 125000 \text{ грн/р.}$$

З відеоспостереженням ймовірність знижується до 1%, тобто збитки:

$$L_{\text{reduced}} = 2500000 \times 0,01 = 25000 \text{ грн/р.}$$

Економія:

$$S_{\text{theft}} = 125000 - 25000 = 100000 \text{ грн/р.}$$

Без відеоспостереження розслідування інцидентів (наприклад, витік інформації чи порушення дисципліни) потребує залучення зовнішніх фахівців, що коштує приблизно 50000 грн/р. З відеоспостереженням ці витрати скорочуються до 10000 грн завдяки швидкому доступу до архіву. Економія:

$$S_{\text{invest}} = 50000 - 10000 = 40000 \text{ грн/р.}$$

За даними Ajax Systems, відеоспостереження підвищує продуктивність працівників на 10–15% за рахунок зниження несанкціонованих перерв і порушень [4]. Для ТОВ «Інноваційні Технології» з річним фондом оплати праці 3000000 грн це дає економію:

$$S_{\text{productivity}} = 3000000 \times 0,12 = 360000 \text{ грн/р.}$$

Загальний економічний ефект:

$$E_{\text{total}} = 100000 + 40000 + 360000 = 500000 \text{ грн/р.}$$

Структура економічного ефекту від впровадження системи показана на рис. 3.1.

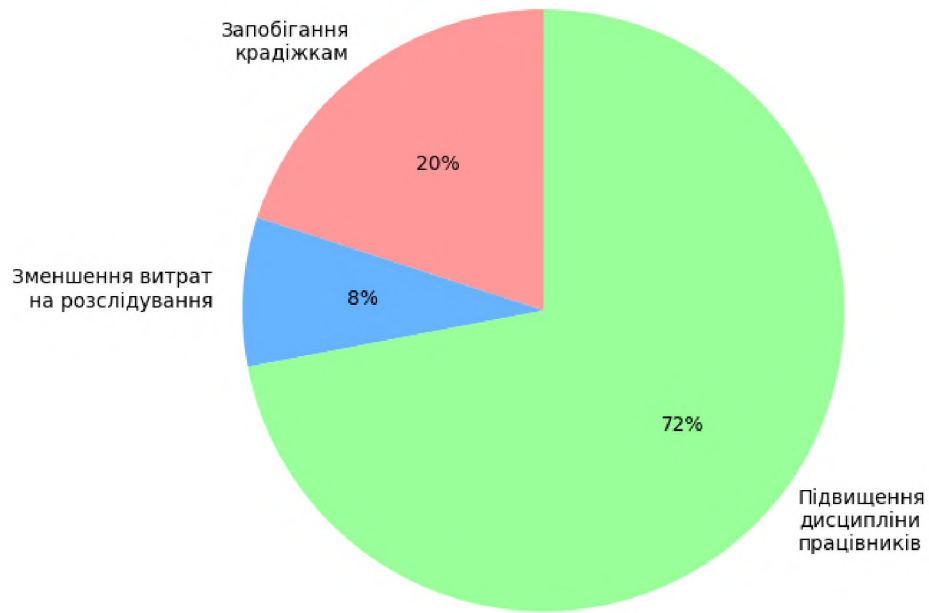


Рисунок 3.1 – Структура економічного ефекту від впровадження системи

Для оцінки окупності використано показник простого строку окупності (Payback Period, PP):

$$PP = \frac{C_{\text{cap}}}{E_{\text{total}} - C_{\text{exp}}}, \quad (3.1)$$

де C_{cap} – капітальні витрати (168380 грн),

E_{total} – річний економічний ефект (500000 грн),

C_{exp} – річні експлуатаційні витрати (25835,73 грн).

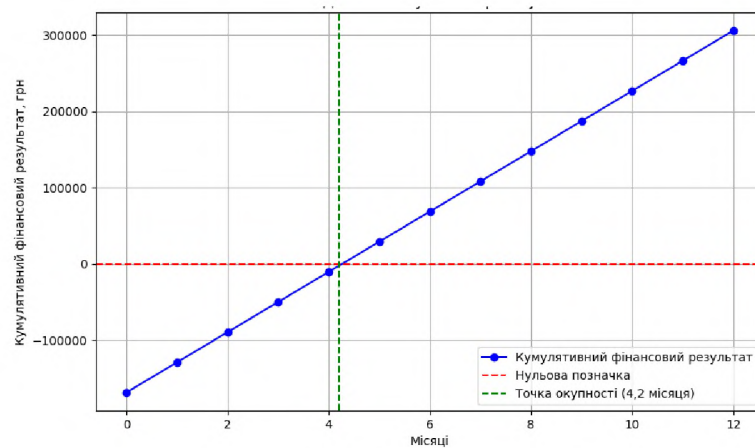


Рисунок 3.2 – Динаміка окупності проекту

Підставляючи значення:

$$PP = \frac{168380}{500000 - 25835,73} \approx 0,35 \text{ р.} \approx 4,2 \text{ міс.}$$

Строк окупності становить приблизно 4,2 місяця, що свідчить про високу економічну ефективність проекту (рис. 3.2). За даними Kyivstar Business Hub, середній строк окупності систем відеоспостереження в офісах становить 6-12 місяців, що підтверджує доцільність впровадження [30].

Для оцінки стійкості проекту до змін зовнішніх умов проведено аналіз чутливості, який враховує можливе зростання експлуатаційних витрат або зниження економічного ефекту. Якщо експлуатаційні витрати зростуть на 20% (до 31002,88 грн/р.), а економічний ефект зменшиться на 20% (до 400000 грн/р.), строк окупності складе:

$$PP_{\text{adjusted}} = \frac{168380}{400000 - 31002,88} \approx 0,46 \text{ р.} \approx 5,5 \text{ місяця.}$$

Навіть у песимістичному сценарії строк окупності залишається в межах 6 місяців, що є прийнятним для інвестицій у системи безпеки. За даними IT Expert, системи відеоспостереження з окупністю до 12 місяців вважаються економічно виправданими для малого та середнього бізнесу [33].

Окрім прямого економічного ефекту, впровадження системи відеоспостереження забезпечує низку непрямих переваг. Наявність сучасної системи безпеки зміцнює довіру клієнтів і партнерів, що особливо важливо для ТОВ «Інноваційні Технології», яка працює з конфіденційною інформацією. За даними Ajax Systems, компанії з розвиненою інфраструктурою безпеки мають на 15% вищу лояльність клієнтів [4]. Деякі страхові компанії надають знижки до 10% на страхування майна за наявності відеоспостереження. Для офісу з вартістю майна 2500000 грн це може заощадити до 25000 грн/р. Відеоаналітика, налаштована для критичних зон (каса, серверна), дозволяє автоматизувати моніторинг, зменшуючи навантаження на службу безпеки. За оцінками Dahua Technology, це може знизити витрати на персонал безпеки на 5-10% [29].

Економічне обґрунтування показало, що впровадження IP-системи відеоспостереження для ТОВ «Інноваційні Технології» потребує капітальних витрат у розмірі 168380 грн і річних експлуатаційних витрат 25835,73 грн. Завдяки зниженню ризиків крадіжок, витрат на розслідування та підвищенню дисципліни працівників річний економічний ефект становить 500000 грн. Строк окупності проекту – 4,2 місяця, що є значно нижчим за середньоринкові показники (6-12 місяців). Аналіз чутливості підтвердив стійкість проекту до змін умов, а додаткові переваги, такі як підвищення репутації та зниження страхових внесків, посилюють його економічну привабливість. Впровадження системи дозволить не лише підвищити безпеку офісу, але й забезпечить швидку віддачу від інвестицій, що відповідає стратегічним цілям підприємства.

3.2 Рекомендації щодо масштабування та модернізації

Масштабування та модернізація IP-системи відеоспостереження для ТОВ «Інноваційні Технології» є важливими аспектами забезпечення довгострокової ефективності системи в умовах зростання підприємства, розширення клієнтської бази та появи нових технологічних рішень. Цей підрозділ містить рекомендації щодо розширення системи до 32 камер, оновлення обладнання, впровадження сучасних технологій, таких як відеоаналітика та хмарні сервіси, а також оцінку витрат на модернізацію. Рекомендації враховують поточну конфігурацію системи та сучасні тенденції в сфері відеоспостереження, що ґрунтуються на аналізі ринку безпеки [16, 29].

Поточна IP-система відеоспостереження включає 12 камер (10 Hikvision DS-2CD2055FWD-I та 2 IMOU Cruiser 2 5MP), мережевий відеореєстратор (NVR) Hikvision DS-7732NI-K4, комутатор D-Link DGS-1210-28P та ДБЖ APC Smart-UPS 1500VA. Система спроектована з урахуванням можливості розширення до 32 камер, що відповідає вимогам замовника. Для масштабування системи необхідно врахувати такі аспекти:

1. Додавання камер. NVR Hikvision DS-7732NI-K4 підтримує до 32 каналів, що дозволяє підключити ще 20 камер без заміни відеореєстратора. Рекомендується використовувати камери Hikvision DS-2CD2055FWD-I для внутрішніх приміщень і зовнішнього периметра завдяки їхній надійності та сумісності з поточною системою. Для зон із обмеженим доступом до кабельної інфраструктури доцільно застосовувати Wi-Fi-камери IMOU Cruiser 2 5MP. Орієнтовна вартість додаткових 20 камер (15 Hikvision по 3 480 грн і 5 IMOU по 3741 грн) становить:

$$C_{\text{cameras}} = (15 \times 3480) + (5 \times 3741) = 52200 + 18705 = 70905 \text{ грн.}$$

2. Мережева інфраструктура. Комутатор D-Link DGS-1210-28P має 24 порти, з яких 15 уже зайнято (10 камер, 2 відеодомофони, NVR, сервер, точка доступу). Для підключення додаткових 20 камер необхідно встановити ще один комутатор, наприклад, D-Link DGS-1210-28P, вартістю 14699 грн. Це забезпечить достатню кількість портів і бюджет PoE (193 Вт) для живлення нових камер [18].

3. Зберігання даних. Поточна ємність жорстких дисків ($4 \times 10 \text{ ТБ} = 40 \text{ ТБ}$) розрахована на зберігання архіву від 12 камер протягом 30 діб. При додаванні 20 камер із роздільною здатністю 5 Мп і стисненням H.265 обсяг даних зросте. Розрахунок додаткового обсягу пам'яті для 20 камер:

$$V = \frac{20 \times 4 \times 24 \times 3600 \times 30}{8 \times 1024^3} \approx 62,2 \text{ ТБ.}$$

Загальний обсяг пам'яті для 32 камер: $37,3 + 62,2 = 99,5 \text{ ТБ}$. Для забезпечення цього обсягу необхідно додати 6 жорстких дисків по 10 ТБ (вартістю 15000 грн кожен), що складе 90000 грн. NVR підтримує до 8 дисків, тому заміна обладнання не потрібна.

4. Енергозабезпечення. ДБЖ APC Smart-UPS 1500VA забезпечує автономність для поточної системи (363 Вт). При додаванні 20 камер ($15 \times 10 \text{ Вт} + 5 \times 12 \text{ Вт} = 210 \text{ Вт}$) загальна потужність зросте до $363 + 210 = 573 \text{ Вт}$. Рекомендується замінити ДБЖ на модель APC Smart-UPS 2200VA (1980 Вт, ціна ~22 000 грн), яка забезпечить автономність до 4 годин [24].

Орієнтовні витрати на масштабування системи наведено в таблиці 3.2.

Таблиця 3.2 – Орієнтовні витрати на масштабування системи до 32 камер

Найменування	Кількість, шт.	Ціна за одиницю, грн	Загальна вартість, грн
Камери Hikvision DS-2CD2055FWD-I	15	3480	52200
Камери IMOU Cruiser 2 5MP	5	3741	18705
Комутатор D-Link DGS-1210-28P	1	14699	14699
Жорсткі диски (10 ТБ)	6	15000	90000
ДБЖ APC Smart-UPS 2200VA	1	22000	22000
Кабелі, короби, монтаж	1	20000	20000
Разом			217604

Загальні витрати на масштабування становлять 217604 грн. Це дозволяє розширити систему без значних змін у поточній інфраструктурі, що відповідає вимогам масштабованості.

Модернізація системи спрямована на впровадження сучасних технологій, таких як розширена відеоаналітика, хмарне зберігання даних і оновлення програмного забезпечення, що підвищить ефективність і безпеку. Основні рекомендації включають:

1. Відеоаналітика. Поточні камери Hikvision DS-2CD2055FWD-I підтримують базові функції відеоаналітики (виявлення руху, перетин лінії). Рекомендується впровадити розширену аналітику, таку як розпізнавання обличчя і номерів автомобілів, для посилення контролю доступу та ідентифікації відвідувачів. За даними Dahua Technology, використання відеоаналітики знижує витрати на охорону на 10–15% завдяки автоматизації моніторингу [29]. Для цього необхідно оновити прошивку камер і NVR, а також придбати ліцензію на програмне забезпечення Hikvision AI Cloud (орієнтовна вартість – 15000 грн/р.).

2. Хмарне зберігання. Для підвищення безпеки даних і доступності архіву рекомендується інтегрувати систему з хмарним сервісом Hik-Connect Cloud. Хмарне зберігання дозволяє створювати резервні копії критичних записів (з каси, серверної) і забезпечує доступ до архіву в разі пошкодження локальних дисків. За даними Kyivstar Business Hub, хмарні рішення знижують ризик втрати

даних на 90% [30]. Орієнтовна вартість хмарного сервісу для 32 камер становить 12000 грн/р. (на основі тарифів Hikvision Cloud). Схема інтеграції хмарного сервісу з IP-системою показана на рис. 3.3.

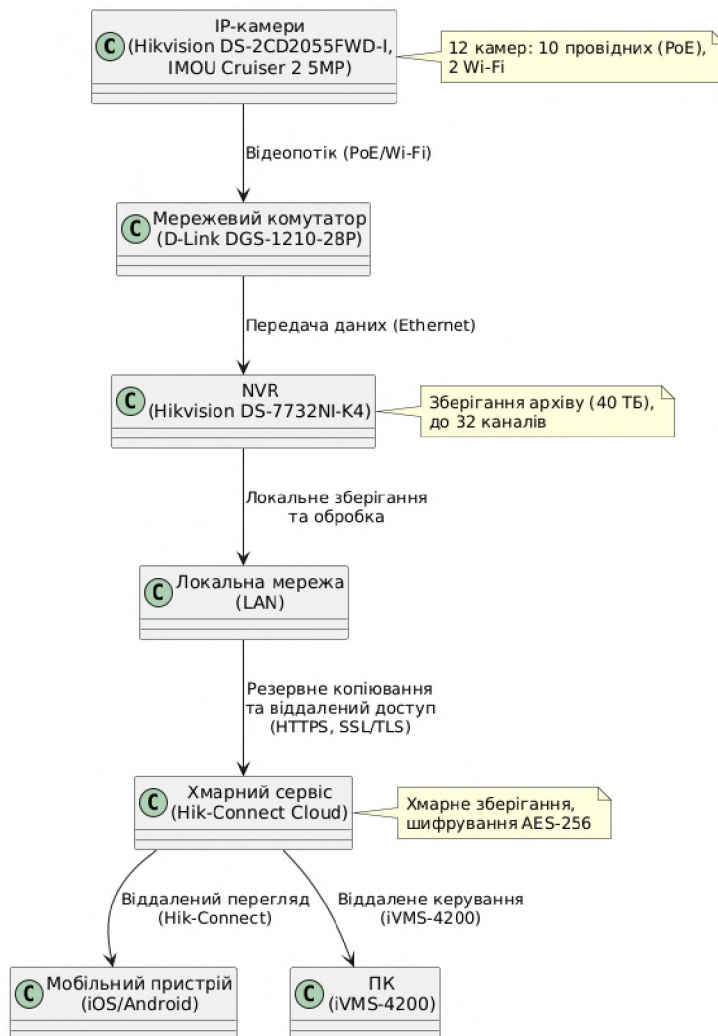


Рисунок 3.3 – Схема інтеграції хмарного сервісу з IP-системою

3. Оновлення програмного забезпечення. Поточне ПЗ Hik-Connect забезпечує базові функції віддаленого доступу. Для розширення функціональності (наприклад, створення аналітичних звітів або інтеграції з CRM-системами) рекомендується перейти на ПЗ HikCentral Professional. Це рішення підтримує управління великими системами відеоспостереження та інтеграцію з іншими системами безпеки. Вартість ліцензії – приблизно 20000 грн одноразово [16].

4. Оновлення обладнання. Через 3-5 років після впровадження рекомендується замінити камери на моделі з підтримкою роздільної здатності 8 Мп і вдосконаленою аналітикою, наприклад, Hikvision DS-2CD2085G1-I (ціна ~4500 грн за одиницю). Це підвищить якість зображення та можливості системи. Орієнтовна вартість заміни 32 камер – 144000 грн.

Впровадження відеоаналітики та хмарного сервісу потребує додаткових витрат, але забезпечує економію за рахунок автоматизації та зниження ризиків. Орієнтовні річні витрати на модернізацію:

- відеоаналітика (Hikvision AI Cloud) – 15 000 грн;
- хмарне зберігання (Hik-Connect Cloud) – 12 000 грн;
- ПЗ HikCentral Professional (одноразово, амортизація на 3 р.) – 6667 грн/р.;

Загалом: $15\,000 + 12\,000 + 6\,667 = 33\,667$ грн/р.;

Економічний ефект від модернізації включає:

- зниження витрат на охорону (10% від річного бюджету на охорону 500000 грн) – 50000 грн/р.;
- запобігання втраті даних (оціночна економія 30 000 грн/р. за рахунок хмарного резервування).

Загальний ефект: $50\,000 + 30\,000 = 80\,000$ грн/р.

Чистий ефект: $80\,000 - 33\,667 = 46\,333$ грн/р.

Модернізація є економічно виправданою, оскільки забезпечує додатковий ефект і підвищує безпеку. За даними Ajax Systems, компанії, що впроваджують відеоаналітику, підвищують ефективність безпеки на 25% [4].

Рекомендації щодо масштабування передбачають додавання 20 камер, нового комутатора, жорстких дисків і потужнішого ДБЖ із витратами 217604 грн. Модернізація включає впровадження відеоаналітики, хмарного сервісу та оновлення ПЗ, що потребує 33667 грн/р., але забезпечує чистий економічний ефект 46333 грн/р. Ці заходи відповідають стратегічним цілям ТОВ «Інноваційні Технології» щодо забезпечення безпеки та підтримки зростання підприємства.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети та виконано всі завдання, спрямовані на створення сучасної IP-системи відеоспостереження для ТОВ «Інноваційні Технології». Було проведено комплексний аналіз теоретичних основ, сучасних технологій, вимог та аналогів, що дозволило розробити ефективну, масштабовану систему відеоспостереження з високою якістю зображення, надійним зберіганням даних і економічною ефективністю.

На етапі теоретичного аналізу досліджено основи систем відеоспостереження та їхню роль у забезпеченні безпеки комерційних об'єктів. Визначено, що IP-системи є ключовим елементом автоматизації охоронних процесів, забезпечуючи високу якість зображення, інтеграцію з іншими системами безпеки та віддалений доступ. Проаналізовано аналогові та цифрові системи, зокрема їхні переваги й недоліки. Зроблено висновок про перевагу IP-систем за якістю зображення, масштабуванням і функціональністю.

Проведено аналіз вимог до системи відеоспостереження, визначено функціональні (покриття критичних зон, аудіозапис, віддалений доступ) та нефункціональні (надійність, масштабованість, безпека) вимоги. Досліджено об'єкт (офіс ТОВ «Інноваційні Технології» площею 250 м²) і його зони безпеки, що дозволило врахувати специфіку приміщень і потенційні загрози. На основі порівняння аналогів обрано обладнання з оптимальним співвідношенням ціна/якість, що забезпечує конкурентні переваги системи завдяки високій роздільній здатності (5 Мп), підтримці PoE і Wi-Fi, а також інтеграції з охоронною сигналізацією та СКУД.

Розроблено архітектуру системи відеоспостереження, яка включає 12 камер, NVR, комутатор і ДБЖ. Розміщення обладнання оптимізовано для максимального покриття зон спостереження, мінімізації «мертвих зон» і захисту від несанкціонованого доступу. Конфігурування системи передбачало налаштування мережевих параметрів, параметрів відеозапису, інтеграцію з

іншими системами безпеки та організацію доступу з розмежуванням прав. Впроваджено заходи безпеки: шифрування AES-256, двофакторну автентифікацію, захист від мережових атак, що забезпечило надійність і безпеку даних.

Практична реалізація системи включала оцінку економічної ефективності. Капітальні витрати склали 168380 грн, експлуатаційні – 25835,73 грн/р.. Економічний ефект від зниження ризиків крадіжок, витрат на розслідування та підвищення дисципліни працівників оцінено в 500000 грн/р., що забезпечує строк окупності 4,2 міс. Аналіз чутливості підтвердив стійкість проекту до змін умов (5,5 міс. в песимістичному сценарії). Додаткові переваги включають підвищення довіри клієнтів і знижки на страхування майна.

Розроблено рекомендації щодо масштабування та модернізації системи. Масштабування до 32 камер потребує витрат 217604 грн і включає додавання камер, комутатора, жорстких дисків і потужнішого ДБЖ. Модернізація передбачає впровадження розширеної відеоаналітики, хмарного зберігання та оновлення ПЗ (33667 грн/р.), що забезпечує чистий економічний ефект 46333 грн/р.

Таким чином, усі поставлені завдання виконано в повному обсязі. Розроблена IP-система відеоспостереження відповідає сучасним вимогам, забезпечуючи високу якість зображення, безпеку даних, зручність використання та економічну ефективність. Напрямами подальших досліджень є вдосконалення відеоаналітики (наприклад, розпізнавання обличчя на основі алгоритмів машинного навчання), інтеграція з платформами IoT для автоматизації безпеки та розширення хмарних функцій. Також необхідно провести тестування системи при максимальному навантаженні (32 камери) для оцінки її масштабованості та стабільності.