

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

**Факультет комп'ютерних наук та технологій**

(повне найменування факультету)

**Кафедра комп'ютерних систем та мереж**

(повне найменування кафедри)

**Пояснювальна записка**

до дипломного проєкту (роботи)

бакалавра

(ступінь вищої освіти (освітній ступінь))

на тему РОЗРОБКА ОХОРОННОЇ СИСТЕМИ  
ТОВ «МІКРОФІНАНС І КОМПАНІЯ»

Виконав: студентка 4 курсу групи КНТ 511сп  
спеціальності \_\_\_\_\_

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація) \_\_\_\_\_

«Комп'ютерна інженерія»

ДРОЗДА К. А.

(ПРИЗВИЩЕ та ініціали)

Керівник ТЯГУНОВА М Ю.

(ПРИЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.

(ПРИЗВИЩЕ та ініціали)

Міністерство освіти і науки України  
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій  
Кафедра «Комп'ютерних систем та мереж»  
Ступінь вищої освіти бакалаврський  
Спеціальність 123 – «Комп'ютерна інженерія»  
(код і найменування)  
Освітня програма (спеціалізація) Комп'ютерна інженерія  
(назва освітньої програми (спеціалізації))

**ЗАТВЕРДЖУЮ**

Завідувач кафедри КУДЕРМЕТОВ Р. К.

«          »            2024 року

**З А В Д А Н Н Я**  
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

Дрозда Катерини Андріївни

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) «Розробка охоронної системи ТОВ «Мікрофінанс і компанія»»

керівник проєкту (роботи) к.т.н. доцент ТЯГУНОВА Марія Юріївна

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «01» квітня 202 року № 105

2. Строк подання студентом проєкту (роботи) 27 травня 2024 року

3. Вихідні дані до проєкту (роботи) Підприємство що має 13 кабінетів на одному поверсі та додаткові кімнати. Необхідно було забезпечити відеоспостереження по всьому поверху, для контролю за роботою, встановити СКУД для унеможливлення проникнення.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз предметної області

Проектування охоронної системи

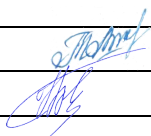
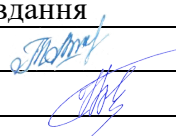
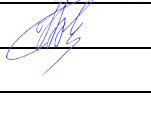
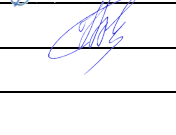
Апаратне та програмне забезпечення

Налаштування роботи системи

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Структурна схема, монтажна схема, Алгоритм роботи сигналізації, програмне забезпечення системи

## 6. Консультанти розділів проєкту (роботи)

| Розділ        | ПРИЗВИЩЕ, ініціали та посада консультанта | Підпис, дата                                                                        |                                                                                     |
|---------------|-------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|               |                                           | завдання видав                                                                      | прийняв виконане завдання                                                           |
| 1-7           | ТЯГУНОВА М.Ю., к. т. н., доцент           |  |  |
| нормоконтроль | ЩЕРБАК Н.В., ст. викл.                    |  |  |
|               |                                           |                                                                                     |                                                                                     |
|               |                                           |                                                                                     |                                                                                     |
|               |                                           |                                                                                     |                                                                                     |
|               |                                           |                                                                                     |                                                                                     |

7. Дата видачі завдання « 23 » лютого 2024 року.

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проєкту (роботи)                | Строк виконання етапів проєкту (роботи) | Примітка |
|-------|---------------------------------------------------------|-----------------------------------------|----------|
| 1     | Аналіз технічного завдання                              | 05.03.2024 р.                           |          |
| 2     | Системи відеоспостереження, охорони та контролю доступу | 05.04.2024 р.                           |          |
| 3     | Проектування мережі                                     | 12.04.2024 р.                           |          |
| 4     | Вибір апаратного забезпечення                           | 20.04.2024 р.                           |          |
| 5     | Вибір програмного забезпечення                          | 26.04.2024 р.                           |          |
| 6     | Налаштування роботи системи                             | 08.05.2024 р.                           |          |
| 7     | Оформлення графічного матеріалу                         | 12.05.2024 р.                           |          |
| 8     | Оформлення пояснювальної записки                        | 20.05.2024 р.                           |          |
|       |                                                         |                                         |          |
|       |                                                         |                                         |          |

Студент(ка)

  
( підпис )

Катерина Дрозда

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

  
( підпис )

Марія Тягунова

(Ім'я ПРИЗВИЩЕ)

## РЕФЕРАТ

ПЗ: 68 стор., рис. 21, посилань 18

ВІДЕОСПОСТЕРЕЖЕННЯ, ВІДЕОРЕЄСТРАТОРИ, ДАТЧИКИ, КАМЕРИ,  
КОНТРОЛЕР, СИГНАЛІЗАЦІЯ, СИСТЕМА КОНТРОЛЮ ДОСТУПОМ,  
ОХОРОНА,

Мета роботи – забезпечити контроль за безпековою ситуацією ТОВ «Мікрофінанс і компанія» за рахунок розробки охоронної системи.

Об’єкт дослідження – офісні охоронні системи.

Предмет розробки – охоронна система ТОВ «Мікрофінанс і компанія»

У першому розділі проведено аналіз технологій підвищення контролю за безпековою ситуацією приміщення: відеоспостереження, охоронні сигналізації та системи контролю доступу, а саме тип відеонагляду - аналоговий або цифровий, СКУД – біометрична, карткова та пінкова.

У другому розділі висунуто вимоги підприємства до системи безпеки. Спроектовано систему охоронної безпеки, яка складається підсистем: відеоспостереження. Контроль та керування доступом, охоронна та пожежна сигналізація. Наведено алгоритми роботи кожної з підсистем та охоронної системи в цілому.

У третьому розділі описано вибір апаратної та програмної складової системи. Для належного функціонування системи згідно висунутих у другому розділі вимог було обрано камери Dahua, реєстратор Hikvision, СКУД Hikvision, охоронна та пожежна сигналізація Ajax. Також обрано таке програмне забезпечення від виробників Hikvision для відеоспостереження та СКУД, додаток Ajax для систем сигналізацій.

У четвертому розділі описано процес налаштування програмної частини охоронної системи для її ефективного функціонування.

## ЗМІСТ

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Вступ.....                                                         | 6  |
| 1 Аналіз предметної області.....                                   | 8  |
| 1.1 Системи відеоспостереження.....                                | 8  |
| 1.2 Відеореєстратори у відеонагляді .....                          | 18 |
| 1.3 Системи контролю доступу.....                                  | 23 |
| 1.4 Системи сигналізації.....                                      | 30 |
| 2 Проєктування охоронної системи .....                             | 37 |
| 2.1 Вимоги до системи.....                                         | 37 |
| 2.2 Структура системи .....                                        | 43 |
| 2.3 Монтажна схема системи .....                                   | 47 |
| 2.4 Функціонування системи.....                                    | 50 |
| 3 Апаратне та програмне забезпечення .....                         | 54 |
| 3.1 Вибір апаратного забезпечення системи .....                    | 54 |
| 3.2 Вибір програмного забезпечення .....                           | 57 |
| 4 Налаштування роботи системи.....                                 | 61 |
| Висновки .....                                                     | 66 |
| Перелік джерел посилання .....                                     | 67 |
| Перелік графічних матеріалів:                                      |    |
| Плакат 1 – Монтажна схема;                                         |    |
| Плакат 2 – Структурна схема;                                       |    |
| Плакат 3 – Зображення апаратного забезпечення;                     |    |
| Креслення 1 – Блок-схема алгоритму роботи підсистеми сигналізації; |    |
| Креслення 2 – Блок-схема алгоритму роботи підсистеми відео.        |    |

## ВСТУП

У сучасному світі питання безпеки є одним з найважливіших аспектів будь-якої компанії. Зростання технологічних можливостей веде за собою збільшення кількості загроз, як внутрішніх так і зовнішніх, які можуть впливати на стабільність та ефективність бізнес-процесів. Враховуючи це, розробка ефективної охоронної системи стає не просто задачею технічного характеру, а стратегічною необхідністю спрямованою на захист активів компанії, даних та персоналу.

Ця дипломна робота спрямована на проєктування та реалізацію комплексної охоронної системи для компанії, яка включатиме в себе сучасні технології та методи захисту. Основна мета проєкту – створення надійного та адаптивного рішення, здатного протистояти потенційним загрозам, мінімізувати ризики та забезпечити безперебійну роботу компанії. Охоронна система представляє собою комплекс заходів і технічних засобів, спрямованих на захист від різних загроз, контроль доступу до важливих ресурсів та інформації, а також реагування на надзвичайні ситуації.

У рамках цієї роботи розглядатимуться такі аспекти як інтеграція систем відеоспостереження, системи контролю доступу, сигналізації, а також розробка політик безпеки і відповідності нормативним вимогам. Крім того, важливим елементом роботи стане аналіз ринку сучасних охоронних систем, їхніх переваг та недоліків, а також вибір оптимального комплексу технічних та програмних засобів, які найкраще відповідають потребам компанії. Особлива увага була приділена вибору відповідних технологій та обладнання, проєктуванню інфраструктури системи, а також її реалізації.

У результаті реалізації даної дипломної роботи очікується отримання моделі охоронної системи, яка буде не тільки ефективно захищати компанію від зовнішніх та внутрішніх загроз, але й слугувати зразком для подальшого впровадження подібних систем в інших організаційних структурах.

Актуальність теми обумовлена зростаючою потребою в забезпеченні високого рівня безпеки в умовах сучасних загроз. Багато компаній стикаються з проблемою несанкціонованого доступу до своїх ресурсів, що може призвести до значних фінансових втрат, витоку конфіденційної інформації та шкоди репутації. Розробка сучасних охоронних систем дозволяє мінімізувати ці ризики та забезпечити стабільну роботу.

Мета роботи – забезпечити контроль за безпековою ситуацією ТОВ «Мікрофінанс і компанія» за рахунок розробки охоронної системи.

Для досягнення поставленої мети необхідно виконати такі завдання:

- провести аналіз технологій підвищення контролю за безпековою ситуацією приміщення;
- розробити вимоги до охоронної системи;
- спроектувати систему згідно висунутих вимог;
- обрати відповідне апаратне та програмне забезпечення системи;
- налаштувати коректну роботу охоронної системи.

## 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

### 1.1 Системи відеоспостереження

Ще в минулому столітті термін «відеоспостереження» міцно закріпився в нашому лексиконі, і він залишається там і зараз. В сучасному світі неможливо знайти підприємство, завод або магазин, який не має камер відеоспостереження. Крім того, у наш час системи відеоспостереження поступово входять і в сферу приватного життя людей. Розглянемо для чого потрібно відеоспостереження.

По-перше відеоспостереження є важливим компонентом сучасних систем безпеки, через великий розвиток злочинності в сучасному суспільстві. Люди все більше прагнуть захистити себе від небажаних вторгнень і посягань на приватність їх життя або особистого майна. Важко уявити надійну систему безпеки без камер відеоспостереження.

Існують зовнішні і внутрішні камери спостереження. Внутрішні камери встановлюють всередині приміщення для того щоб спостерігати за ситуацією всередині об'єкта, а зовнішні дозволяють охороняти прилеглу територію об'єкта будь то приватне володіння, завод склад чи магазин. Сучасні камери спостереження можуть виявляти та розпізнавати людей на відстані кількох десятків метрів. Також існують камери які можуть рахувати кількість людей які проходять певну межу встановлену на камері. Крім того, інфрачервоне підсвічування, яке є частиною більшості вуличних камер відеоспостереження, дозволяє спостерігати за подіями навіть у повній темряві.

Внутрішні камери відеоспостереження стали більш поширеними. Наприклад, в магазинах вони дозволяють стежити за крадіжкою, не тільки з боку клієнтів, але й з боку працівників. Практика показує, що після встановлення систем відеоспостереження злочинність в магазині зменшується на 70-80%. Це стосується не тільки магазинів але й будь якої організації, будь то складські виробничі, торгові чи будь-які інші організації. Внутрішні відеокамери дозволяють керівникам компанії постійно стежити за роботою своїх підлеглих.

Причому можна зробити це за допомогою відеоспостереження в інтернеті будь якої точки земної кулі.

Сучасні IP-камери відеоспостереження дозволяють створювати аудіо зв'язок між тим, хто спостерігає та об'єктом спостереження, що спрощує процес керівництва над персоналом.

Багато людей встановлюють внутрішні відеокамери в приватних будинках і квартирах для охорони не тільки прилеглої території та периметру власного будинку, але й усередині житла з метою спостереження за персоналом якого наняли за нянькою для дитини, гувернанткою або за іншими членами своєї родини.

Встановлені камери відеоспостереження в дитячих садках, школах та інших навчальних закладах дозволяють батькам спостерігати за тим, чим займається їхнє улюблене дитя, а також стежити за тим, як проходять заняття в групі або уроки в класі, в будь який час.

Як ми бачимо не тільки слово «відеоспостереження» давно стало частиною нашого лексикону, але й самі системи відеоспостереження стали важливою частиною нашого життя. Усі сфери життєдіяльності людини потребують відеокамер, моніторів і відеореєстраторів.

Розвиток технологій відеоспостереження, незважаючи на будь-які досягнення не може бути зупинено. Сьогодні відеоспостереження, як і багато інших комп'ютеризовані технології, активно перетворюється на автоматизовані інтелектуальні рішення, які використовують машинний зір, інтернет ресурси, елементи доповненої реальності та багато чого іншого.

У середині минулого століття з'являються перші системи відеоспостереження (рис. 1.1). З тих пір вони розвиваються разом з іншими технологіями, які використовуються для збору, накопичення та обробки інформації. Еволюція складається з кількох етапів:

- поява перших примітивних систем нагляду: на початку XX століття перші камери були створені для ведення спостереження в охоронному та воєнному контексті. Ці системи використовували аналогові засоби та зберігали відеозапис

на фізичних носіях, таких як плівка та магнітна стрічка;

- епоха аналогових систем: в середині XX століття почали з'являтися аналогові системи відеонагляду, які використовували аналогові камери та відеореєстратори для запису відеопотоку. Ці системи були широко застосовані в охороні об'єктів та громадських місць;

- перехід на цифрові системи: на кінці XX століття та початку XXI століття цифрові технології почали витісняти аналогові системи. Цифрові камери відеоспостереження надавали кращу якість зображення, були більш гнучкими та мали здатність передавати відеопоток через мережу;

- інтеграція мережевих технологій: з розвитком мережевих технологій, таких як Інтернет та Ethernet, системи відеонагляду стають все більш і більш інтегрованими з комп'ютерними мережами. Це надало доступ до віддаленого доступу до відеопотоку, а також інтеграцію з іншими системами безпеки та керування;

- впровадження штучного інтелекту та аналітики: сучасні системи відеонагляду набагато частіше використовують технології штучного інтелекту й аналітики для автоматичного пошуку та аналізу подій. Це включає в себе такі функції як розпізнавання обличчя, пошук руку, класифікацію об'єктів та прогнозування поведінки;

- хмарні технології та мобільні додатки: з розвитком хмарних технологій системи відеонагляду стали більш доступними та гнучкими. Збереження відеопотоку на хмарі дозволяє віддалений доступ та керування відеокамерами через мережу інтернет. А мобільні додатки дають доступ до простого моніторингу камер в будь якій точки світу.



Рисунок 1.1 – Перша камера відеоспостереження

Хоч сьогодні камери спостереження можна побачити на кожному кроці, ще не так давно це було можливо тільки на державних об'єктах. Системи безпеки стають все більш популярними. Відео контролює повсякденне життя.

Основна функція камери полягає в тому, щоб знімати зображення, розділяти їх на кілька нерухомих кадрів і рядків, передавати їх і швидко відтворювати їх на екрані. Завдяки цьому людське око сприймає зображення як рухоме. Вибираючи телекамеру, ми повинні брати до уваги багато функцій, залежно від застосування, деякі з них дуже важливі, інші не так важливі. Використовуючи інструкції, неможливо судити про камери за одним або двома параметрами.

Зазвичай, основні завдання камери в системі відеонагляду включають такі функції:

- спостереження і фіксація подій: основне завдання камери полягає в спостереженні за об'єктом або територією і фіксація подій, які відбуваються в області її огляду. Камера записує відео або зображення для подальшого аналізу або збереження;
- забезпечення безпеки: камери відеонагляду використовують для

забезпечення безпеки об'єктів, приміщень, території та осіб. Вони дозволяють вчасно виявляти потенційні загрози, викрадення, вторгнення або інші небажані події;

- моніторинг працівників: камери можуть використовуватися для контролю за працівниками на робочих місцях, щоб спостерігати за їхньою діяльністю, дотриманням правил безпеки та внутрішніх процедур;

- виявлення порушень правил і норм: відеокамери також допомагають виявляти порушення правил та норм, такі як паркування на заборонених місцях, проїзд на червоне світло, вторгнення на заборонені території тощо;

- допомога в розслідуванні подій: відеозаписи, зняті камерами, можуть використовуватися в якості доказового матеріалу під час розслідування злочинів або інцидентів;

- захист майна і майнових цінностей: допомагають захищати майно від крадіжок, вандалізму та інших пошкоджень, сприяючи вчасному виявленню та відслідковуванню потенційних загроз;

- сприяння і підвищенні ефективності процесів і безпеки: завдяки камерам можна виявляти слабкі місця в процесах роботи, розробляти ефективніші стратегії безпеки та управління що допомагає підвищити загальну ефективність підприємства чи організації.

Різні виробники використовують різні стандарти та підходи до оцінки, і навіть якщо знати як прочитати всі цифри в технічному паспорті, все одно потрібно оцінити якість зображення, порівнюючи його з зображенням з іншої камери. У більшості випадків порівняльний тест є найкращим і єдиним об'єктивним методом оцінки характеристик камери, таких як вертикальний ореол, шум, чутливість тощо. Загальне враження про хорошу якість зображення створюється комбінацією багатьох чинників: роздільної здатності, ореолу, чутливості, шуму, гамма-корекції та інших. Людське око не однаково чутливе до всіх цих факторів.

Основні характеристики камер відеонагляду визначають їхню функціональність, якість зображення та можливості. Розглянемо деякі з

найважливіших характеристик, таких як:

- чутливість;
- роздільна здатність;
- об'єктив (фокусна відстань і кут огляду);
- функція підсилення зображення;
- функції інтелектуального аналізу;
- ІЧ-підсвічування;
- ступінь водонепроникності та механічного захисту;
- підтримка віддаленого доступу.

Чутливість до світла і темряви, ця характеристика вказує на те, наскільки добре камера може записувати чіткі зображення навіть при слабкому освітленні або в умовах ночі. Це досягається за допомогою спеціальних сенсорів і об'єктивів, а також застосуванням технологій підвищення чутливості.

Роздільна здатність камери визначає кількість деталей, які вона може зафіксувати на зображенні. Вона вимірюється в кількості пікселів (горизонтальної та вертикальної ліній), наприклад, 1920x1080 пікселів для Full HD або 3840x2160 пікселів для 4K Ultra HD. Чим вище роздільна здатність, тим більше деталей можна розрізнити на зображенні.

Фокусна відстань вказує на те, наскільки далеко камера може збільшувати об'єкт. Вона визначається в мм і залежить від типу об'єктива. Кут огляду показує широкість зони, яку камера може охопити. Він може бути фіксованим або регульованим. Залежно від потреб застосування, можна вибрати об'єктив з певною фокусною відстанню і кутом огляду.

Функція підсилення зображення - деякі камери мають функції підсилення зображення, такі як зум, фокусування, функція повороту або нахилу. Вони дозволяють коригувати зображення в реальному часі і отримувати більш чіткі та деталізовані результати.

Функції інтелектуального аналізу сучасні камери можуть мати вбудовані функції інтелектуального аналізу, такі як виявлення руху розпізнавання облич, зони виявлення та інші. Ці функції дозволяють автоматично виявляти та

реагувати на певні ситуації, спрощуючи процес моніторингу та аналізу відеоданих.

ІЧ-підсвічування дозволяє камері знімати відео в умовах темряви або при дуже слабкому освітленні, використовуючи інфрачервоне світло. Це важлива характеристика для нічного спостереження, яка дозволяє отримувати якісні зображення навіть в умовах обмеженого освітлення;

Ступінь водонепроникності та механічного захисту - для камер, які встановлюються ззовні, важливою є ступінь їхньої водонепроникності та механічного захисту. Вони можуть мати вбудовані корпуси, які захищають від пилу, вологи та вандалів, що забезпечує надійну роботу камери в умовах зовнішнього середовища;

Підтримка віддаленого доступу - деякі камери можуть підтримувати збереження записів на внутрішньому накопичувачі або в хмарних сервісах, а також підтримують віддалений доступ через мобільні додатки або веб-інтерфейси. Це дозволяє користувачам переглядати відео в реальному часі та отримувати доступ до записів з будь-якого місця, де є інтернет-з'єднання.

Ці характеристики допомагають вибирати камеру відеонагляду, яка найкращим чином відповідає вашим потребам і вимогам конкретного застосування.

Існує кілька видів камер відеонагляду, кожен з яких має свої особливості і використовується в різних ситуаціях. Ось найпоширеніші типи камер:

- фіксовані камери;
- PTZ (Pan-Tilt-Zoom) камери;
- IP (Internet Protocol) камери;
- аналогові камери;
- бездротові камери;
- приховані (шпигунські) камери;
- теплові камери.

Фіксовані камери ці камери мають фіксований об'єктив і не можуть змінювати свого положення, вони охоплюють одну сталу область. Вони

найчастіше використовуються для нагляду за статичними об'єктами або територіями, такими як входи, коридори або приміщення. Їх встановлюють на стіні або стелі, і вони залишаються на місці протягом тривалого часу без необхідності регулярного налаштування.

PTZ (Pan-Tilt-Zoom) камери ці камери мають можливість повороту (панорама), нахилу (тільт) та збільшення (зум) об'єктива. Вони дозволяють операторам віддалено керувати напрямком та збільшенням об'єкта. Це забезпечує широкий діапазон огляду і може бути використано для відстеження об'єктів у реальному часі, таких як рухомі транспортні засоби або особи.

IP (Internet Protocol) камери передають відеосигнал через мережу інтернет, що дозволяє отримувати доступ до відео з будь якої точки з інтернет з'єднанням. Зазвичай мають різні роздільні здатності, вбудовані функції аналізу та інші характеристики.

Аналогові камери камери які використовують аналогове з'єднання для передачі відеосигналу до монітора або записуючого пристрою. Вони більш дешеві у встановленні, але зазвичай мають меншу роздільну здатність і функціональність порівняно з IP-камерами.

Бездротові камери ці камери підключаються до мережі бездротового зв'язку, що дозволяє їх встановлювати у віддаленому або важкодоступних місцях. Вони зазвичай простіші в установці, оскільки не потребують проводів для передачі сигналу, але можуть мати обмежену дальність передачі сигналу.

Приховані (шпигунські) камери ці камери зазвичай мають мініатюрний розмір і приховані в об'єктах або предметах, таких як кульки, ручки або прикраси. Вони використовуються для таємного стеження або безпеки.

Теплові камери камери використовують інфрачервоне випромінювання для створення зображення на основі теплового випромінювання об'єктів. Вони можуть виявляти теплові плями, людей або тварин у темряві або в умовах обмеженого видимого світла.

Відеонагляд можна вести за допомогою відкритих або прихованих відеокамер. Такі камери створюються таким чином, щоб об'єкт спостереження не

міг бачити, що вони знімаються. Приховану камеру можна помістити в будь який предмет, наприклад в книгу або м'яку іграшку. Також випускають приховані камери об'єktiv якої за розмірами меншу ніж сірникова головка. Такі камери називають «пінхол» (pinhole), в перекладі це означає «шпилька в отворі», такі камери встановлюють прямо в стіну, щоб лише об'єktiv цієї камери було видно на поверхні. Камера відеоспостереження може бути направлена в одну точку, або змінювати кут огляду, якщо вона має поворотний механізм. За рахунок того, що вони можуть повертати об'єktiv і фіксувати події навколо них, так звані поворотні камери практично не мають «сліпих зон» спостереження. Ці пристрої зручно використовувати для керування великими площами, такими як автостоянки або супермаркети. Поворотна функція дозволяє зменшити кількість камер відеонагляду, одночасно збільшуючи площу огляду на об'єкті спостереження. Практично всі поворотні камери мають функцію наближення зображення, ця функція буде корисною у разі якщо вам потрібно детально розглянути якийсь об'єкт на відео. Також багато поворотних камер можна налаштувати на певну послідовність повороту об'єктива. Це можна зробити за допомогою налаштувань, в яких потрібно вказати періодичність і кут повороту камери. Окрім різноманітних типів камер, описаних вище, існують також модульні відеокамери. Це міні-камери з електронною платою та оптичним об'єktivом. Для запобігання забруднення таких камер, як правило потрібно придбати спеціальні захисні чохла, кожухи або корпуси.

Одним з основних характеристик розподілу камер спостереження є їхнє місце розташування, тож камери поділяють на внутрішні і зовнішні. Вуличні камери мають свою специфіку, оскільки такі камери призначені для вуличного спостереження їх вмонтовують в спеціальний термо-кожух, для того щоб різка зміна погодних умов не вивела камеру з ладу. Крім того цей кожух захищає камеру від пилу та вологи, також на деяких камерах вказують ступінь їх захисту, наприклад IP-66, то перша цифра вказує на пилонепроникність а друга про вологозахист.

Зовні камери також можуть значно відрізнитись. Одним з найбільш цікавих

прикладів цієї відмінності є купольні та стандартні камери відеоспостереження (рис 1.2, та 1.3).



Рисунок 1.2 - Купольні камери спостереження



Рисунок 1.3 - Стандартні камери

Мініатюрна камера спостереження являє собою камеру, укладену в скляний тонований купол, який приховує від сторонніх очей, в який бік в даний момент спрямований об'єктив. Кріпиться купольна камера до стелі як правило в центрі приміщення для забезпечення огляду на 360 градусів. Звичайна стандартна камера відеоспостереження, яка виглядає як прямокутний пристрій з об'єктивом, подивившись на таку камеру можна вже приблизно знати що потрапляє до її об'єктиву.

Всі камери описані вище, мають аналоговий тип передачі сигналу. Це

означає, що запис зроблений такою камерою оцифровується не відразу. Оцифрування відеозапису відбувається після передачі сигналу з відеокамери на записуючий пристрій, тільки після цього є можливість записати готовий відеопотік на жорсткий диск. В даний час все більше починають використовувати мережеві камери, також відомі як IP- камери. Ці камери самостійно оцифровують сигнал, така функція дозволяє відправляти отримані відеозаписи за допомогою Інтернету на будь-яку вибрану адресу без попередньої передачі даних без попередньої передачі даних на відеосервер. Зазвичай така функція мережевих камер тягне за собою витрачання частини необхідного для підприємства інтернет-трафіку, тому при використанні даного виду камер необхідно буде витратити час на оптимізацію використовуваного мережевого ресурсу. Також іноді використовують фальшкамери, або муляжі камер, ці камери використовують лише для видимості, і виконують функцію тільки психологічного впливу на об'єкт.

## **1.2 Відеореєстратори у відеонагляді**

Відеореєстратори – це пристрої, які призначені для запису та зберігання відеофайлів з камер спостереження.

Неможливо уявити професійну систему відеоспостереження без такого компонента як відеореєстратор. Він дозволяє значно розширити функціонал камер, навіть якщо вони вважаються повністю автономними пристроям. Крім того відеореєстратор допоможе правильно організувати зберігання даних.

Якщо дивитись на цифро-аналогове відеоспостереження, то в такій системі наявність відеореєстратора (рис 1.2) є обов'язковою умовою. Робота камер без нього буде неповноцінною.

До додаткових переваг використання відеореєстратора можна віднести можливість підключення додаткового обладнання, таких як наприклад монітори

для спостереження за камерами в реальному часі, панель керування, звукове обладнання та завдяки встановленому відеореєстратору можна інтегрувати датчики охоронної сигналізації.



Рисунок 1.2 – Цифровий та мережевий відеореєстратор

Еволюція відеореєстраторів тісно пов'язана з розвитком технологій відеоспостереження та зберігання даних. Можна виділити основні моменти розвитку відеореєстраторів опираючись на основні моменти розвитку систем відеоспостереження:

- аналогові відеореєстратори (DVR);
- цифрові відеореєстратори (DVR);
- мережеві відеореєстратори (NVR);
- гібридні відеореєстратори (HVR);
- інтелектуальні відеореєстратори.

Аналогові відеореєстратори (DVR) перші відеореєстратори були аналоговими та використовували магнітні стрічки для запису відео, вони мали обмежену ємність та якість запису, а також були незручними у використанні через необхідність зміни стрічок.

Цифрові відеореєстратори (DVR) з появою цифрових технологій з'явилися цифрові відеореєстратори, які записували відео на жорсткі диски, це дозволило збільшити ємність зберігання, покращити якість запису та спростити процес

пошуку та перегляду відео.

Мережеві відеореєстратори (NVR) розвиток IP-камер призвів до появи мережевих відеореєстраторів, які призначені для роботи з цифровим відеопотоком, що передається через мережу, NVR мають ширші можливості порівняно з DVR, такі як підтримка більшої кількості камер, вища роздільна здатність запису, віддалений доступ та інтелектуальні функції аналізу відео.

Гібридні відеореєстратори (HVR) як перехідний етап між аналоговими та цифровими системами з'явилися гібридні відеореєстратори, які можуть працювати як з аналоговими, так і з IP-камерами, це дозволяє поступово модернізувати систему відеоспостереження, замінюючи аналогові камери на цифрові без необхідності зміни відеореєстратора.

Інтелектуальні відеореєстратори сучасні відеореєстратори все частіше оснащуються функціями штучного інтелекту та машинного навчання, що дозволяє їм автоматично аналізувати відеодані, виявляти події та розпізнавати об'єкти, це значно розширює можливості відеоспостереження та робить його більш ефективним інструментом безпеки.

Вибір найкращого відеореєстратора є важливим кроком у створенні ефективної системи відеонагляду. Різноманітність моделей та функціонал можливостей дозволяє підібрати оптимальне рішення для конкретних потреб та бюджету. Основні критерії вибору відеореєстратора включають :

- кількість каналів;
- роздільна здатність запису;
- швидкість запису;
- обсяг жорсткого диска;
- наявність інтелектуальних функцій;
- підтримка віддаленого доступу.

Кількість каналів — визначає скільки камер можна підключити до відеореєстратора.

Роздільна здатність запису — впливає на якість зображення та обсяг дискового простору, необхідного для зберігання.

Швидкість запису – визначає кількість кадрів за секунду, що записуються для кожної камери.

Обсяг жорсткого диска – впливає на тривалість зберігання відеоархіву.

Наявність інтелектуальних функцій – залежить від потреб бюджету.

Підтримка віддаленого доступу – важлива для моніторингу системи з будь-якого місця.

Існує кілька типів відеореєстраторів, кожен з яких має свої особливості та призначення.

Аналогові відеореєстратори або DVR (Digital Video Recorder), використовують аналогові сигнали з камер спостереження, вони перетворюють ці сигнали в цифровий формат для зберігання файлів на жорсткому диску. Аналогові системи це доступний варіант для базових систем відеоспостереження, яка працює з аналоговими камерами.

Особливостями аналогових реєстраторів полягає в:

- запис відеофайлів на жорсткий диск;
- обмежена якість зображення.

Запис відеофайлів на жорсткий диск запис відео здійснюється на жорсткий диск, що забезпечує зручність та надійність зберігання даних.

Обмежена якість зображення аналогові системи мають обмежену роздільну здатність запису, приблизно до 960x480 пікселів.

До переваг аналогових систем відносять їх невисоку вартість, тому що аналогові системи зазвичай дешевші в обслуговуванні та встановленні, та легкість в налаштуванні. Але й є недоліки – це обмежена функціональність, вона нижча ніж в цифрових системах, та менша якість зображення.

Цифрові відеореєстратори (DVR) – цифрові відеореєстратори також називаються DVR, але використовують цифрові камери спостереження які можуть забезпечувати кращу якість зображення та додаткові функції.

Особливості цифрових систем є:

- підвищена роздільна здатність;
- має більш розширені функції – виявлення руху, оповіщення та

інтелектуальний аналіз відео.

Підвищена роздільна здатність – система може підтримувати високу роздільну здатність відео до Full HD або навіть 4K.

Особливості цифрових систем в цілому є і її перевагами над аналоговими, але через свої переваги вона і отримана недолік – цифрові системи стали дорожчими в установці та обслуговуванні в порівнянні з аналоговими.

Мережеві відеореєстратори або NVR (Network Video Recorder) призначені для роботи з IP-камерами, які передають відео через мережу.

Мережеві системи мають свої переваги:

- віддалений доступ – доступ до відео через інтернет;
- висока роздільна здатність -до 4K та вище;
- гнучкість – легко масштабується та інтегрується з іншими системами безпеки.

Переваги таких систем полягають в тому, що вони мають найкращу якість зображення серед усіх типів систем та мають доступ до відео з будь-якої точки, завдяки віддаленому доступу.

Але в цих системах є і свої недоліки, такі як: висока вартість, яка буде найвищою серед усіх мереж, та вимагають більшої кваліфікації для встановлення та обслуговування.

Гібридні відеореєстратори, або HVR (Hybrid Video Recorder), такі відеореєстратори можуть працювати як з аналоговими так і з цифровими IP-камерами, що робить їх універсальними. Такі реєстратори дозволяють поступово переходити з аналогових систем на цифрові. Перевагою такого типу реєстраторів є економічність, через економію бюджету на поступовому переході з одного типу системи на інший. Але через їх універсальність вони мають недолік – складніша в налаштуванні через підтримку різних типів камер.

### 1.3 Системи контролю доступу

Система контролю та управління доступом (скорочено СКУД або СКД) – комплекс програмно- технічних засобів і організаційних заходів на об’єкті, які дозволяють контролювати та керувати відвідуванням окремих приміщень та оперативно контролювати переміщення персоналу та час його перебування на об’єкті.

Системи контролю управління доступом можуть бути класифіковані за різними ознаками, такими як тип ідентифікації, спосіб передачі сигналу, рівень інтеграції та іншими параметрами.

Залежно від типу контролю доступу системи СКД можуть бути централізованими та автономними.

Централізовані системи включають в себе контролери, які об’єднані в одну мережу та підключені до комп’ютера, який виконує загальне керування. Відеоспостереження, пожежа, та охоронна сигналізація є частиною наявних систем. Централізовані мережі розміщують на великих офісних та промислових об’єктах, які часто приймають велику кількість людей. Одночасно система дозволяє керувати великою кількістю пунктів пропуску, вносити зміни до програми та додавати нові функції.

Автономні системи можуть самостійно керувати периферійними елементами та визначати точки доступу. Використовуються в приватних будинках, громадських та освітніх установах. Банківська сфера часто використовує автономні системи СКУД, для того щоб обмежити доступ до банкоматів, унеможливаючи встановлення скіммерів (спеціальних пристроїв, які зчитують реквізити банківської картки клієнтів). Безпосередньою перевагою автономних систем управління ка контролю доступом є помірна вартість та простота установа, легке керування та надійність в експлуатації.

Також існує біометрична система СКУД, вона ґрунтується на ідентифікації індивідуальних параметрів користувача (сітчатки ока, відбиток пальця) Вона

забезпечує вищий рівень захисту, ніж системи доступу з картками, оскільки біометричні дані не можливо підробити. Переваги цього типу системи полягає в тому що відбувається майже моментальна перевірка особистості та зберігання журналу подій, а її основним мінусом є вартість та неможливість видати тимчасову перепустку.

Системи керування доступом можна поділити на 4 класи:

- перший – мінімальний;
- другий – середній;
- третій – високий;
- четвертий – найвищий.

Перший рівень - проста автономна система, яка дозволяє контролювати доступ до магазину, офісу або іншого приміщення. Час відвідування та інші деталі в такій системи не записуються. Усім співробітникам видається перепустка (картка пропуск), необхідно дати контролеру зчитати код з ідентифікатора для того щоб пройти через турнікет. Оскільки ідентифікація відвідувача виконується за однією ознакою, СКУД цього класу однорівневі. Ідентифікатори з дозволом на вхід можна додавати або видаляти з бази, використовуючи ключ-карту, максимум можна додати близько 2800 осіб. СКУД першого класу оснащені звуковою або світловою ідентифікацією роботи.

Другий рівень-системи керування доступом другого класу як і наступні можуть бути централізованими та багаторівневими, а не лише автономними та однорівневими. Хоча вони забезпечують більший високий рівень безпеки, їх зазвичай використовують як додатковий захист. Можливий функціонал СКД другого класу – це можливість регулювання допуску осіб, тобто власники обраних ідентифікаторів можуть входити на територію, що охороняється лише у визначений час, також можуть фіксувати час у який працівники входять або виходять із закритої зони, ця інформація автоматично зберігається в буфері пам'яті системи керування доступом. Також можлива подача тривожного сигналу на пост охорони або інші пристрої у разі несанкціонованого доступу

Третій рівень являє собою велику мережу пристроїв контролю доступу

розраховану на 1500+ осіб. Однак точок доступу контролерів може бути встановлено не більше ніж 64. Для забезпечення повного рівня безпеки на об'єкті достатньо буде СКУД 3го класу. Система керування доступом 3го класу може виконувати функціонал попереднього, але значно його розширити, наприклад використовувати спеціальний модуль для інтеграції з протипожежних систем та мережею відеоспостереження. Є можливість вести детальний облік кожного відвідувача, включаючи час входу та виходу. Також в системі 3го класу є постійна самодіагностика цілісності складових системи.

Четвертий рівень - використовується на великих об'єктах. По суті це система керування доступом 3го класу тільки з більшою кількістю точок контролерів, понад 64 точки. Може інтегруватись з системою безпеки на програмному рівні, також пристрої загородження керуються автоматично в разі надзвичайної ситуації (такої як пожежа).

Класифікація за типом ідентифікації:

- карткові системи;
- проксіміт – картки;
- смарт- картки;
- сканери відбитків пальця;
- розпізнавання облич;
- розпізнавання райдужки ока;
- розпізнавання голосу;
- пін-кодові системи;
- мобільні рішення.

Карткові системи – використовують магнітні смужки для зберігання ідентифікаційних даних, прикладом є банківські картки(рис. 1.4).

Проксіміт – картки – використовують радіочастотну ідентифікацію, така картка не потребує прямого контакту із контролером.

Смарт- картки – мають вбудований мікрочіп, що зберігає ідентифікаційні дані та може виконувати криптографічні операції.

Сканери відбитків пальця – використовують унікальний малюнок відбитків

пальців для ідентифікації користувача.

Розпізнавання облич – використовують алгоритм комп’ютерного зору для ідентифікації користувача за його обличчям.

Розпізнавання райдужки ока – використовують унікальний малюнок райдужки ока для ідентифікації.

Розпізнавання голосу – використовують унікальні характеристики голосу для ідентифікації.

Пін-кодові системи – використовують цифрові або алфавітно-цифрові коди для ідентифікації користувачів.

Мобільні рішення – використовують технології NFC або Bluetooth для ідентифікації користувачів через мобільні пристрої.



Рисунок 1.4 – Карткова система

Системи керування доступом також поділяють на три категорії за типом передачі даних:

- провідні системи;
- безпроводні системи;
- гібридні системи.

Провідні системи – використовують дротові поєднання між датчиками, зчитувачами контролерами та сигнальними пристроями.

Безпроводні системи – використовують радіозв'язок або інші бездротові технології для передачі сигналів між компонентами системи.

Гібридні системи – поєднують в собі дротові та бездротові технології для забезпечення максимальної гнучкості та надійності системи.

Також системи контролю та управління доступом розподіляють за їх призначенням, тобто існує фізичний контроль доступу, який направлений на обмеження або надання доступу до фізичних приміщень, та логічний контроль доступу, який спрямований на обмежений доступ до комп'ютерних систем, мереж та даних.

Механізм роботи системи контролю доступу досить простий. Кожен працівник, клієнт або відвідувач компанії отримує електронний ключ (пластикову картку) з індивідуальним кодом. Реєстрація перерахованих осіб за допомогою інструментів системи призводить до отримання «електронних ключів». Персональна електронна картка містить інформацію про власника електронного ключа (може включати в себе дані паспорту людини) . Персональна електронна картка власника, та код його електронного ключа зв'язуються один з одним і заносяться в спеціально організовані комп'ютерні бази даних.

Сучасні системи контролю можуть вести облік робочого часу персоналу, це є додатковою перевагою цих систем. Для обліку робочого часу необхідний комплекс програмного забезпечення та апаратних засобів. Програмне забезпечення дозволяє керувати відвідуваністю, створювати онлайн- моніторинги та отримувати декілька варіантів звітів про відвідуваність.

До складу СКД відносять два основні елементи це ідентифікатор та контролер (рис. 1.5). Ідентифікатор – це ключовий елемент, що встановлює право доступу особи на підконтрольну територію підприємство. Цю функцію можуть виконувати :

- картка з магнітною смужкою;
- безконтактна картка;

- спеціальний брелок;
- цифровий код, що безпосередньо вводиться на клавіатурі;
- унікальні особисті ознаки людини (відбитки пальця, долоні, сітківка ока).



Рисунок 1.5 – Компоненти системи СКУД

Спеціальний пристрій зчитує інформацію (модифікація залежить від типу ідентифікатора) та передається у контролер для подальшої обробки. Зазвичай зчитувальні пристрої виконують з урахуванням вимог підвищеного опору механічним впливам.

Контролер – сам приймає рішення про надання чи заборону доступу на основі отриманих даних. Він може працювати самостійно або з іншими пристроями під керування комп'ютера, залежно від типу системи. Для того щоб контролер міг працювати безперервно, він може бути забезпечений блоком резервного живлення або акумулятором. Для подальшого використання, такого як складання звітів, статистика та облік робочого часу, отримана інформація від ідентифікатора зберігається в пам'яті системи.

Системи контролю управління доступом пройшли довгий шлях еволюції, від простих механічних замків до складних електронних та біометричних систем. Їх розвиток був тісно пов'язаний з технологічними досягненнями та зростаючими потребами у безпеці.

Еволюція складається з кількох етапів:

- ранні етапи;
- розвиток електронних систем;
- сучасні технології.

До ранніх етапів можна віднести появу перших механічних замків, які з'явилися ще в стародавньому Єгипті близько 4000 років тому, вони були виготовлені з дерева. Пізніше в середньовіччі з'явилися більш складні металеві механізми з ключами. Ще пізніше в 19 столітті з'явилися перші кодові замки, вони використовувалися в банках і в інших місцях де було необхідно забезпечити високий рівень безпеки.

Розвиток електронних систем у 1960-х роках компанія IBM розробила технологію магнітних карток, вони використовувалися для банкоматів і швидко знайшли застосування в системах доступу. У 1980-х роках почали з'являтися проксіміт-картки які використовували радіочастотну ідентифікацію, вони не вимагали безпосереднього контакту зі зчитувачем і могли зчитувати інформацію на відстані кількох сантиметрів.

Сучасні технології – у 1990-х роках у використання почали входити смарт-картки, вони забезпечували вищий рівень безпеки через використання в них криптографічних ключів. У 2000-х роках з розвитком технологій в експлуатація почали вводити біометричні системи з розпізнаванням відбитку пальця, обличчя та сітчатки ока. З поширенням смартфонів у 2010-х роках почали з'являтися мобільні додатки для контролю доступом, вони використовували технологію NFC або Bluetooth.

## 1.4 Системи сигналізації

Одним з найкращих сучасних способів забезпечити безпеку будинку або підприємства є охоронна сигналізація. Ця система реагує на підозрілу активність або спроби зламати двері. Охоронні сигналізації відмінні тим що вони можуть сповіщати про спробу втручання на приватну територію або аварію яка відбулась пожежа або затоплення водою.

Основними компонентами систем сигналізації є:

- датчики та сенсори(рис.1.6);
- контролери сигналізації;
- сигнальні пристрої;
- комунікаційні модулі.



Рисунок 1.6 – Датчики та сенсори сигналізації

До датчиків та сенсорів можуть відносити:

- датчики руху;

- датчики дверей та вікон;
- датчики розбиття скла;
- пожежні датчики;
- датчики витоку газу;
- датчики затоплення.

Датчики руху – виявляють рух у контрольованій зоні за допомогою інфрачервоного випромінювання, ультразвуку або мікрохвиль.

Датчики дверей та вікон - реагують на закриття та відкриття вікон або дверей за допомогою магнітних контактів.

Датчики розбиття скла – реагують на звуки або вібрації, які виникають при розбитті скла.

Пожежні датчики – виявляють дим, підвищену температуру або вогонь.

Датчики витоку газу – виявляють наявність небезпечних газів у повітрі.

Датчики затоплення – реагують на наявність води на підлозі.

Контролери сигналізації включають в себе центральні пристрої, які збирають дані від датчиків та сенсорів, обробляють їх та приймають рішення про спрацювання сигналізації, а також мають можливість підключення до зовнішніх систем для передачі сигналів тривоги (наприклад, на пульт охорони або мобільний додаток).

Сигнальні пристрої:

- сирени та світлові індикатори;
- тривожні кнопки.

Сирени та світлові індикатори – видають гучні звукові і світлові сигнали у разі спрацювання системи.

Тривожні кнопки – ручні пристрої, які дозволяють активувати сигналізацію у разі небезпеки.

Комунікаційні модулі це пристрої для передачі сигналів тривоги на віддалені пристрої або служби (наприклад через GSM, інтернет або радіоканал) вони забезпечують можливість віддаленого моніторингу та управління системою сигналізації.

Сигналізація має чотири основні функції:

- виявлення загроз;
- оповіщення про загрози;
- реєстрація подій;
- інтеграція з іншими системами безпеки.

Виявлення загроз – системи сигналізації забезпечують своєчасне виявлення різних видів загроз (проникнення, пожежа, пожежа, витік газу, затоплення).

Оповіщення про загрози – сигналізація активує звукові і світлові сигнали, попереджаючи про небезпеку як всередині об'єкта так і ззовні (наприклад, на пульті охорони або мобільному додатку).

Реєстрація подій – системи сигналізації ведуть журнал подій, записуючи всі випадки спрацювання та їх характеристики. Це дозволяє аналізувати інциденти і вживати заходи для запобігання подібним ситуаціям у майбутньому.

Інтеграція з іншими системами безпеки – сигналізація може бути інтегрована з системами відеоспостереження, контролю доступу та іншими охоронними системами для створення комплексного захисту.

Розвиток систем сигналізації був тісно пов'язаний з потребами суспільства в забезпеченні безпеки та технологічними інноваціями. Системи пройшли розвиток від простих механічних пристроїв до складних інтелектуальних систем, що використовують сучасні технології, системи сигналізації стали невід'ємною частиною нашого повсякденного життя. Основні етапи розвитку даних технологій:

- механічні сигналізації;
- електромеханічні сигналізації;
- сигналізації з проводовим з'єднанням;
- перші охоронні сигналізації;
- перші пожежні сигналізації;
- безпроводні системи сигналізації;
- інтелектуальні системи;
- інтернет речей (IoT);

- біометричні системи;
- штучний інтелект та машинне навчання.

Механічні сигналізації – перші системи сигналізації також були винайдені в стародавньому Єгипті. Вони використовувались для оповіщення про проникнення, вони використовували дзвони та шнури, які активувались при відкритті воріт або дверей. У середньовіччі використовували більш складний механізм із ланцюгами замість шнурів.

Електромеханічні сигналізації – з винайденням електрики були завірені перші патенти на електромеханічні сигналізації, однією з перших була система яка використовувала електричний струм для активації дзвона при відкритті дверей або вікон.

Сигналізації з проводовим з'єднанням – поява телеграфу і телефону на початку 20-х років відкрила нові можливості для сигналізації, провідні системи почали використовувати для передачі сигналу тривоги на віддалені пункти охорони або поліцію.

Перші охоронні сигналізації – після другої світової війни у 1950-х роках розвиток електроніки привів до появи перших охоронних сигналізацій, які включали в себе датчики руху, сирени та магнітні контакти на вікнах та дверях.

Перші пожежні сигналізації – у 1960-х роках з'явилися перші пожежні сигналізації, що включали в себе датчики диму та тепла, вони встали обов'язковими для встановлення в багатьох країнах.

Безпроводні системи сигналізації – розвиток радіо технологій у 1980-х роках дозволив створити безпроводні системи сигналізацій, які використовували радіосигнали для передачі тривожних повідомлень між компонентами системи.

Інтелектуальні системи – у 2000-х роках впровадження мікропроцесорів і програмного забезпечення дозволив створювати інтелектуальні системи сигналізації, які могли аналізувати дані з декількох датчиків, визначати тип загрози і приймати відповідні рішення.

Інтернет речей (IoT) – використання інтернету дозволило об'єднувати системи сигналізації з хмарними сервісами, забезпечуючи віддалений доступ та

керування.

Біометричні системи – використання біометричних технологій, таких як розпізнавання облич, відбитків пальців, дозволяє створювати більш надійні та персоналізовані системи.

Штучний інтелект та машинне навчання – використання алгоритмів штучного інтелекту і машинного навчання для аналізу даних з датчиків і відеокамер дозволяє виявляти загрози більш точно та ефективно.

Системи сигналізації є важливими елементами забезпечення безпеки різних об'єктів, від приватних будинків до великих промислових підприємств. Вони можуть бути класифіковані за різними критеріями, такими як типи загроз, які вони виявляють, спосіб передачі сигналів, рівень інтеграції з іншими системами та інші параметри. Системи сигналізації є критичними компонентами забезпечення безпеки в різних сферах діяльності. Їх різноманітність дозволяє вибрати оптимальне рішення для конкретних умов і вимог, забезпечуючи ефективний захист від широкого спектру загроз.

За способом передачі сигналу системи сигналізації поділяються так само як і системи керування доступу:

- провідні системи;
- безпроводні системи;
- гібридні системи.

Провідні системи – датчики, контролери та сигнальні пристрої пов'язані між собою дротовим з'єднанням. Їх застосовують у великих будівлях, промислових об'єктах, які потребують високої надійності.

Безпроводні системи – компоненти системи передають зв'язок через радіосигнал або інші бездротові технології. Ці технології використовують в невеликих офісах приватних будинках, квартирах та об'єктах з обмеженими можливостями для прокладання кабелів.

Гібридні системи – поєднують в собі провідні та безпроводні системи для того щоб максимізувати надійність та гнучкість систем. Їх використовують у великих торгових центрах, бізнес центрах та в державних установах.

Другий тип класифікації сигналізаційних систем за типом захищеності об'єктів, до них відносять:

- охоронні сигналізації;
- пожежні сигналізації;
- газові сигналізації;
- системи затоплення.

Охоронні сигналізації – призначені для виявлення несанкціонованого доступу до об'єктів. До їх основного складу входять датчики розбиття скла, магнітні контакти на вікна та двері та датчики руху. В основному їх використовують у житлових будинках, офісах магазинах та складах.

Пожежні сигналізації – призначені для пошуку пожеж та швидкого сповіщення про них. В їх склад входять димові, теплові та комбіновані датчики, а також ручні пожежні сповіщувачі. Їх застосовують у всіх типах будівлях.

Газові сигналізації – працюють за таким же принципом як і пожежні, тільки різниця в тому, що реагують на витіки газу, а не вогню. До їх складу входять датчики метану, пропану та чадного газу. Ці системи використовують на кухнях, в котельних та газових приміщеннях.

Системи затоплення – призначені для пошуку води в місцях, де її не повинно бути, до складу цих систем входять датчики затоплення, в основному їх використовують в підвалах, кімнатах серверів та складських приміщеннях.

Наступний тип класифікації – це класифікація за методом виявлення загроз поділяють на два типи, перший тип це -активні система, яка використовує активні сенсори, які випромінюють сигнали та аналізують їхні відбиття до їхнього складу входять мікрохвильові та ультразвукові датчики, друга - пасивна система використовує пасивні сенсори, що не випромінюють сигналів, для реагування на зміни в навколишньому середовищі, до їх складу зазвичай входять димові датчики та пасивні інфрачервоні датчики.

Останній тип класифікації систем – за рівнем їхньої інтеграції:

- автономні системи;
- інтегровані системи.

Автономні системи – можуть працювати не залежно від інших встановлених систем та мають власні вбудовані сигнальні пристрої.

Інтегровані системи – інтегруються в вже наявні охоронні та інформаційні системи для комплексного захисту.

Класифікація за типом реакції на небезпеку:

- автономна;
- пультова;
- GSM.

Автономна сигналізація – працює самостійно не потребує підключення до зовнішньої мережі або не потребує контролю оператора. Вона може мати датчики диму, дверей, вікон та руху. Сирена активується системою. Коли пристрій спрацює. Така модель зазвичай використовується в будинках або інших місцях, де власник не має постійного контролю.

Пультова сигналізація – усе обладнання керується за допомогою пульта керування, за його допомогою власник може вмикати та вимикати сигналізацію та стежити за станом об'єкта. Зазвичай вони встановлюються в комерційних приміщеннях або будинках, де є необхідність в цілодобовому керуванні та контролі (рис 1.7).

- GSM сигналізація – автономна сигналізація, яка може передавати інформацію за допомогою технології GSM. Оскільки не потрібно прокладати кабелі її установка займає меншу часу та зусиль порівняно з провідними аналогами. Крім того власник системи може отримувати повідомлення за допомогою мобільної мережі.



Рисунок 1.7 – Пультова сигналізація

## 2 ПРОЄКТУВАННЯ ОХОРОННОЇ СИСТЕМИ

ТОВ «Мікрофінанс і компанія» - це фінансова установа, яка надає послуги з мікrokредитування населенню. Як і інші фінансові установи, компанія отримує та зберігає готівку, конфіденційні фінансові дані своїх клієнтів та цінне майно компанії (офісне обладнання, комп'ютерна техніка та інше). Це робить компанію потенційно привабливою мішенню для злочинної діяльності, такої як крадіжка, вандалізм, шахрайство та несанкціонований доступ до компанії. Окрім можливості незаконного впливу людини, компанія як і будь-які інші підприємства можуть піддаватись ризику пожежі, потопу або витоків газу та інших надзвичайних ситуацій, які можуть загрожувати безпеці працівників, та зазнати значної шкоди.

Враховуючи ці фактори, впровадження системи безпеки є необхідним засобом для компанії. Система безпеки дозволить:

- забезпечити безпеку співробітників;
- захистити матеріальні цінності;
- запобігти витоків конфіденційної інформації;
- своєчасно виявляти та реагувати на надзвичайні ситуації.

Таким чином, система безпеки не тільки підвищує рівень безпеки офісу, але і сприяє створенню більш комфортного та надійного середовища для співробітників.

### 2.1 Вимоги до системи

Аналіз вимог є критично важливим етапом у процесі розробці охоронної системи, оскільки він закладає основу для всіх подальших кроків у проєктуванні та впровадженні систем. Детальний та ретельний аналіз дозволить в подальшому

врахувати всі особливості об'єкта, потенційні загрози для нього, законодавчі вимоги і побажання замовника, що в результаті забезпечує створення ефективної та надійної системи безпеки.

Мені необхідно було визначити необхідні заходи для забезпечення безпеки персоналу, матеріальних цінностей та інформації. Офіси часто є місцями з високою концентрацією людей і цінних активів, що робить їх привабливим для зловмисників. Тому мною був проведений аналіз основних аспектів вимог для охоронної системи офісу. Аналіз потенційних загроз:

- тип об'єкта;
- потенційні загрози;
- вандалізм;
- пожежі;
- витоки газу;
- затоплення.

Тип об'єкта – офісне приміщення – офісні будівлі включають в себе окремі кабінети, конференц-зали, робочі зони відкритого планування кімнати для відпочинку, архіви, серверні кімнати, тощо. Їх особливість полягає в тому що в такому типі приміщення висока кількість працівників та відвідувачів, велика кількість дорогого обладнання, важливість захисту конференційної інформації;

Потенційні загрози – проникнення та крадіжки – зловмисники можуть проникнути в офіс для викрадення обладнання або конфіденційної інформації;

Вандалізм – пошкодження майна або обладнання;

Пожежі – пожежі можуть виникнути через несправність електрообладнання або через людський фактор;

Витоки газу – витоки газу можуть призвести до вибухів або отруєння персоналу;

Затоплення – затоплення можуть виникнути через водопровід або систему опалення.

Також не менш важливим було звернути увагу на законодавчі вимоги для правомірного функціонування офісного приміщення та його співробітників, що

включає в себе :

- пожежну безпеку ;
- захист персональних даних.

Пожежна безпека – система повинна відповідати нормам і стандартам пожежної безпеки, включаючи вимоги щодо встановлення датчиків диму і тепла, систем пожежогасіння, евакуаційних шляхів згідно з ДБН В2.5-56:2014 «Системи пожежної сигналізації та оповіщення»;

Захист персональних даних – система повинна забезпечувати захист персональних даних співробітників та клієнтів відповідно до законодавства, згідно із Закону України «Про захист персональних даних»;

Згідно з функціональними вимогами, система безпеки повинна включати в себе:

- систему контролю доступу;
- систему відеоспостереження;
- систему охоронної сигналізації;
- пожежну сигналізацію;

Система контролю доступу – встановлення системи контролю доступу для обмеження доступу до приміщень на основі ідентифікаційних карток. Контроль входу і виходу, реєстрація відвідувань, управління доступом до окремих зон.

Система відеоспостереження – встановлення камер відеоспостереження у ключових точках (входи, коридори, серверні кімнати, зони зберігання цінностей тощо). Моніторинг ситуації в реальному часі, запис відео для подальшого аналізу.

Система сигналізації – встановлення охоронної сигналізації, яка включає датчики руху. Розбиття скла, відкриття дверей та вікон. Виявлення і оповіщення про спроби несанкціонованого доступу.

Пожежна сигналізація – встановлення пожежних датчиків і систем автоматичного пожежогасіння. Виявлення пожежі, автоматичне сповіщення, активація систем пожежогасіння.

Також вона повинна мати наступні характеристики:

- продуктивність;

- надійність;
- масштабованість;
- вартість обладнання;
- витрати на встановлення;
- витрати на обслуговування.

Продуктивність – система повинна забезпечувати високу швидкість обробки даних і реагування на загрози;

Надійність – система повинна бути надійною і стійкою до збоїв, з можливістю резервного живлення і захисту від фізичного впливу;

Масштабованість – система повинна мати можливість масштабування для подальшого розширення або модернізації;

Вартість обладнання – оцінка вартості необхідного обладнання, включаючи камери, датчики, контролери. Порівняння вартості різних постачальників і вибір оптимального за співвідношенням ціни та якості;

Витрати на встановлення – оцінка витрат на встановлення і налаштування системи, включаючи оплату праці фахівців. Планування етапів встановлення та залучення кваліфікованих підрядчиків;

Витрати на обслуговування – оцінка поточних витрат на технічне обслуговування і оновлення системи. Вартість річного обслуговування, заміна компонентів, оновлення програмного забезпечення.

Необхідно було відповідати встановленим цілям та вимогам, а саме:

а) цілі:

- 1) забезпечення безпеки співробітників та клієнтів;
- 2) захист матеріальних цінностей компанії (обладнання документи, готівка);
- 3) запобігання несанкціонованого доступу до приміщень та інформації;
- 4) своєчасне виявлення та реагування на позаштатні ситуації (пожежі, витоки газу тощо);

б) обмеження:

- 1) бюджетні обмеження на впровадження та обслуговування системи;
- 2) необхідність мінімізації впливу на повсякденну діяльність компанії під час встановлення системи;
- 3) врахування особливостей приміщень та інфраструктури компанії.

На підставі аналізу вимог можна визначити наступні оптимальні технічні рішення для охоронної системи ТОВ «Мікрофінанс і компанія», які в подальшому забезпечать всім необхідним вимогам та стандартам:

а) система контролю доступу :

- 1) вибір технології;
- 2) обладнання;
- 3) програмне забезпечення;

б) система відеоспостереження:

- 1) вибір камер;
- 2) розміщення камер;
- 3) відеореєстратор;
- 4) моніторинг;

в) охоронна сигналізація:

- 1) вибір датчиків;
- 2) контрольна панель;
- 3) сповіщення;
- 4) пульт охорони;

г) пожежна сигналізація:

- 1) вибір датчиків;
- 2) контрольна панель;
- 3) сповіщення;

д) додаткові рекомендації:

- 1) резервне живлення;
- 2) регулярне обслуговування;
- 3) навчання персоналу.

Вибір технології – використання безконтактних смарт- карток для

забезпечення високого рівня безпеки та зручності використання.

Обладнання – встановлення електромагнітних замків на входах до приміщень, зчитувачів карток даних біля дверей та контролерів для керування доступом.

Програмне забезпечення – використання спеціалізованого програмного забезпечення для управління системою контролю та управління доступом, реєстрації подій, формування звітів.

Вибір камер – встановлення IP- камер з високою роздільною здатністю (Full HD або вище), функцією нічного бачення (ІЧ-підсвічування) та можливістю віддаленого доступу.

Розміщення камер – розміщення камер на входах, виходах, у коридорах, кабінетах, серверних приміщеннях та інших ключових зонах.

Відеореєстратор – використання мережевого відеореєстратора (NVR) для запису, зберігання та управління відеоархівом.

Моніторинг – організація роботи оператора для перегляду відео в реальному часі та доступом до архіву.

Вибір датчиків – встановлення датчиків руху, відкриття дверей та вікон, розбиття скла у всіх приміщеннях, та встановлення димових та теплових датчиків у всіх приміщеннях згідно з вимогами пожежної безпеки.

Контрольна панель – використання контрольної панелі для управління системою, налаштування зон охорони та оповіщення тривоги, та використання контрольної панелі для управління системою та оповіщення про пожежу.

Сповіщення – налаштування сповіщень про тривоги через сирену, світлові індикатори, SMS-повідомлення або push-сповіщення на мобільні пристрої відповідальних осіб, а також налаштування гучних звукових сповіщень та світлових сигналів для сповіщення про пожежу.

Пульт охорони – розгляд можливості підключення системи до пульта централізованого спостереження охоронної компанії».

Резервне живлення – забезпечення резервного живлення для всіх компонентів охоронної системи на випадок відключення електроенергії.

Регулярне обслуговування – проведення регулярного технічного обслуговування та перевірки працездатності системи.

Навчання персоналу – проведення інструктажу співробітників щодо правил користування системою та дій у разі тривоги.

## 2.2 Структура системи

Охоронна система компанії ТОВ «Мікрофінанс і компанія» складається з чотирьох основних підсистем, кожна з яких виконує свою функцію та не залежить одна від одної (рис. 2.1).

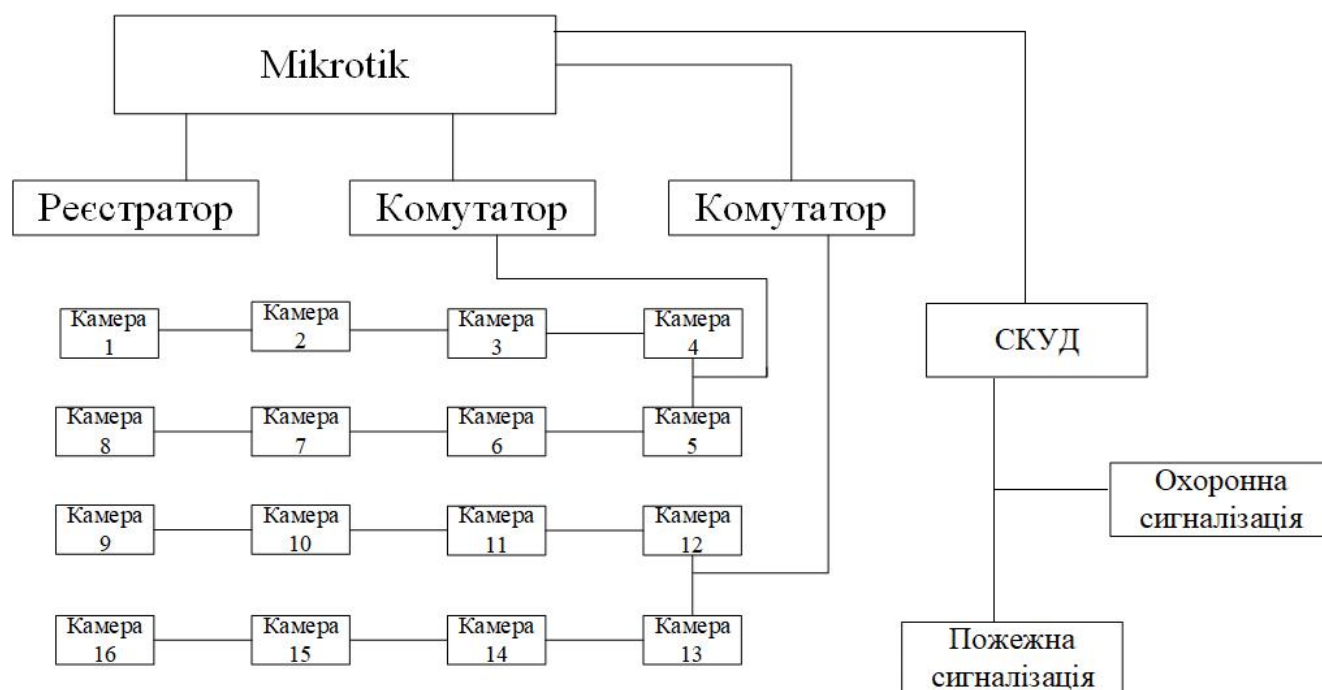


Рисунок 2.1 – Структурна схема охоронної системи

До складу підсистеми відеоспостереження входять:

- 16 IP-камер;
- 2 Рое-комутатори на 8 портів;
- 1 мережевий відеореєстратор на 16 портів.

Камери розташовані по всій території офісу, включаючи входи, виходи, коридори та кабінети, забезпечуючи цілодобовий моніторинг. Мережевий відеореєстратор здійснює запис відео, зберігання та керування відеоархівом, з усіх 16-ти камер, забезпечуючи можливість перегляду та аналізу усіх подій.

До системи контролю та управління доступом входять (рис 2.2):

- зчитувачі;
- електронні замки;
- контролери.

Зчитувачі розміщені біля вхідних дверей, вони забезпечують ідентифікацію співробітників за допомогою карток. Електронні замки встановлені на дверях, керуються завдяки сигналам від зчитувачів, забезпечуючи доступ до приміщення для ідентифікованих осіб. Контролери управляють роботою зчитувачів та замків, обробляють дані про доступ та передають їх на центральний пульт управління.

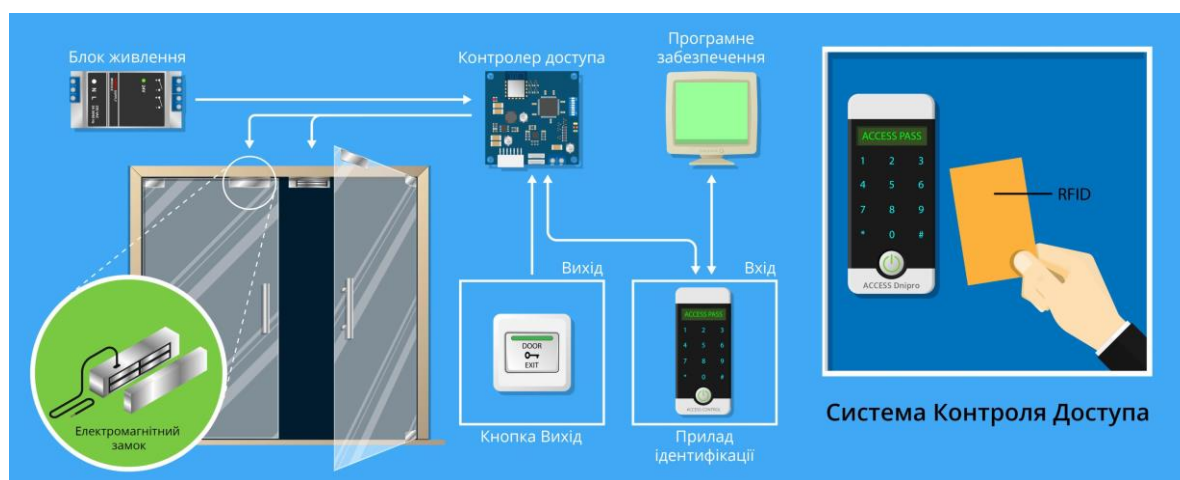


Рисунок 2.2 – схема системи СКУД

Центральний пульт керування системою контролю доступу є головним елементом всієї системи, який об'єднує між собою всі компоненти та забезпечує їхню ефективну функціональність. Він може бути реалізований як окремий пристрій або програмне забезпечення. До основних функцій центрального пульта входять:

- пульт отримує дані із зчитувачів, аналізує їх та перевіряє на відповідність із базою користувачів;
- на основі результатів аутентифікації пульт керування приймає рішення про доступ або заборону входу;
- пульт збирає інформацію про всі події системи, фіксує час та деталі кожної події, та зберігає всі отриманні дані;
- на основі зібраної інформації можливо формувати звіти, такі як час приходу або уходу співробітника, кількість спроб несанкціонованого доступу, статистику використання системи;
- дозволяє налаштувати параметри доступу для різних користувачів, тимчасові доступи та тривалість часу відкритих дверей.

Охоронна сигналізація включає в себе:

- датчики відкриття;
- датчики розбиття скла;
- тривожна кнопка;
- панель управління.

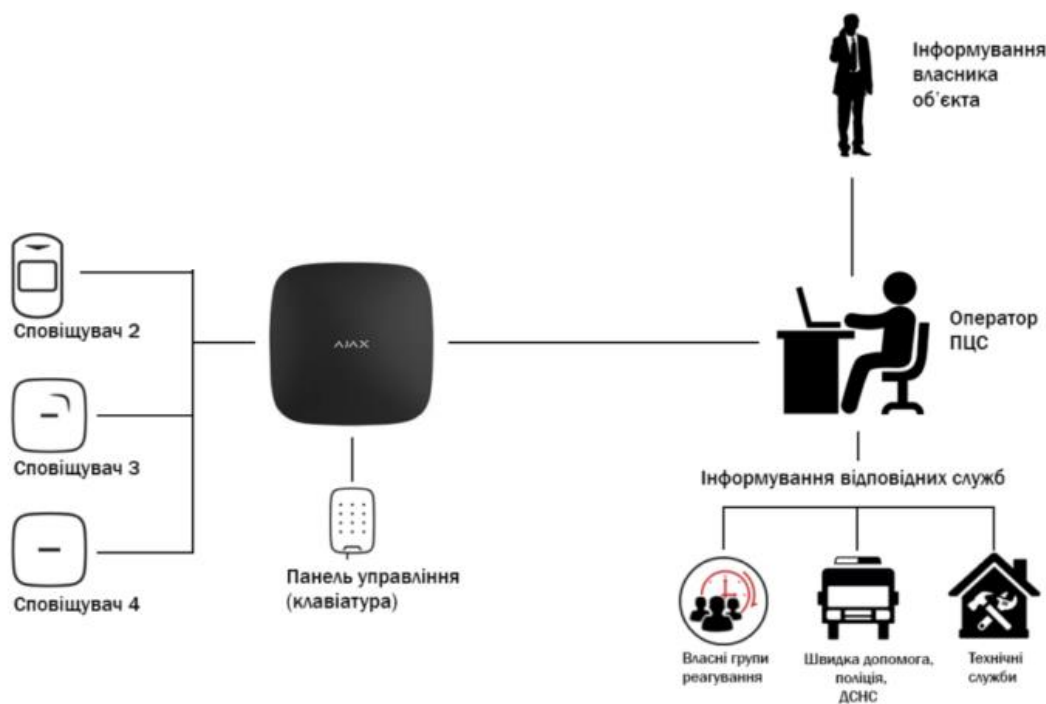


Рисунок 2.3 – схема охоронної сигналізації

Датчики відкриття дверей встановлені на вході та реагують на відкриття дверей поза робочим часом. Датчики розбиття скла встановлені на вікнах, реагують на звук розбиття скла, попереджаючи про спробу проникнення. Тривожна кнопка знаходиться у вповноваженої людини, її використовують у разі надзвичайних ситуацій. Панель управління знаходиться на вході в приміщення, використовують для встановлення на сигналізацію на кінці робочого дня та для зняття з неї на початку.

До складу пожежної сигналізації входить:

- димові та теплові датчики;
- ручні сповіщувачі.

Димові та теплові датчики розміщені по всьому офісу, реагують на появу диму або підвищення температури, що свідчить про можливу пожежу. Ручні сповіщувачі встановлені в зручних місцях, що дозволяє співробітнику вручну активувати сигнал тривоги у разі виявлення пожежі.

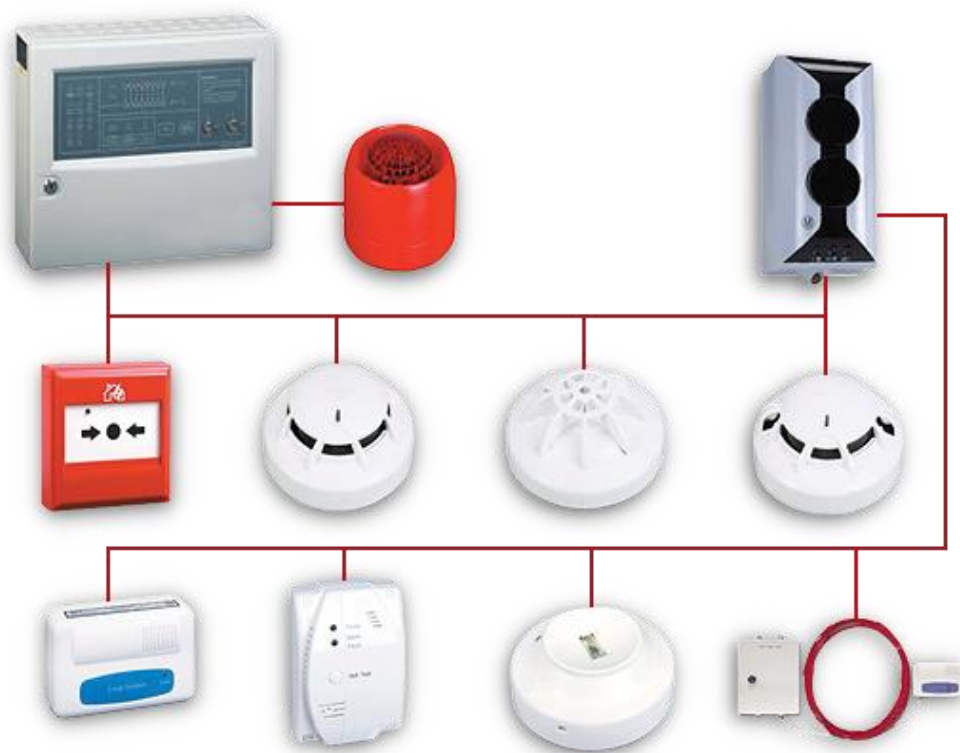


Рисунок 2.4 – структурна схема пожежної сигналізації

## 2.3 Монтажна схема системи

Монтажна схема охоронної системи є важливим документом. Вона буде використовуватись під час встановлення та налаштування системи, а також для її подальшого обслуговування та модернізації. Схема відображає візуально з'єднання всіх частин охоронної системи в офісі.

Монтажна схема являє собою план приміщення офісу (рис. 2.5) з позначенням місць встановлення камер спостереження, відеореєстраторів, датчиків руху, відкриття дверей та вікон контрольних панелей та всіх інших компонентів системи.

Монтажна схема є важливим інструментом для:

- планування та встановлення;
- налаштування та обслуговування;
- модернізації.

Планування та встановлення – дозволяє визначити оптимальне розташування компонентів системи та спланувати маршрути прокладання кабелів.

Налаштування та обслуговування – полегшує процес налаштування та діагностики системи. А також допомагає швидко виявити та усунути несправності.

Модернізація – спрощує внесення змін до системи у разі її розширення або зміни потреб у безпеці.

Наявність детальної та зрозумілої монтажною схемою є запорукою успішного впровадження та ефективної роботи системи

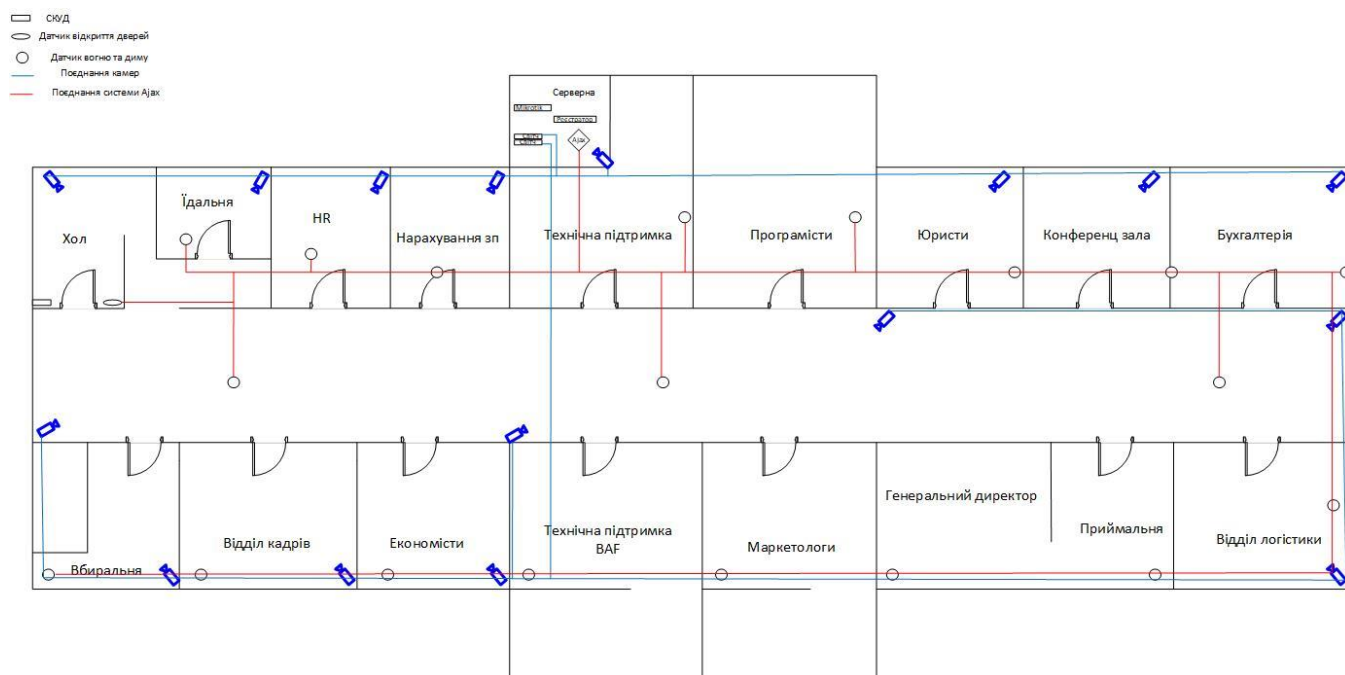


Рисунок 2.5 – Монтажна схема приміщення

#### Опис схеми підключення:

- камери відеоспостереження – розташовані на входах та виходах, в коридорах, кабінетах;
- датчики відкриття дверей і вікон – дверей встановлені на входах, вікон на кожному вікні;
- датчики вогню – встановлюються у всіх приміщеннях відповідно до вимог пожежної безпеки;
- панель керування – розміщена на вході до поверху;
- відеореєстратор – встановлений у безпечному місці із обмеженим доступом.

Камери відеоспостереження встановлені в коридорах, кабінетах та на входах до приміщень через те що є необхідність контролю за переміщенням людей та запобіганню несанкціонованого доступу до приміщень. Таке розташування камер є стратегічно важливим для забезпечення безпеки персоналу, матеріальних цінностей та конфіденційної інформації.

Коридори є ключовим способом переміщення співробітників, тому встановлення камер у цих місцях дозволяє відстежувати переміщення людей,

виявляти підозрілу активність та забезпечувати загальний контроль за ситуацією в офісі.

Кабінети, потребують додаткового захисту. Камери в кабінетах допомагають запобігти крадіжкам, витоку інформації та іншим неправомірним діям.

Входи – найбільш вразливі місця для несанкціонованого доступу. Шляхом встановлення камер на вході та виході відбувається ідентифікація відвідувачів, контроль доступу до приміщення та фіксація спроби проникнення злочинців.

Встановлення СКУД є важливим пунктом у забезпеченні комплексної безпеки компанії, оскільки ця система дозволяє вирішити одразу декілька завдань. Встановлення системи контролю та управління доступом було обумовлено наступним:

- забезпечити безпеку персоналу та матеріальних цінностей;
- контроль робочого часу;
- підвищення рівня безпеки.

Забезпечити безпеку персоналу та матеріальних цінностей є важливим для фінансових установ які працюють з готівкою та конфіденційними даними клієнтів потенційно привабливі для злочинців, тому система СКУД дозволяє обмежити доступ до приміщень лише для ідентифікованих людей, запобігаючи проникненню злочинців.

Контроль робочого часу – керівником компанії було висунуто бажання мати статистику робочого часу ( запізнення, раніше пішли до дому, час перекуру працівника і т.д), система керування доступом дозволить отримати таку статистику, що в подальшому допоможе підвищити дисципліну та оптимізувати робочий процес.

Підвищення рівня безпеки – наявність системи керування доступом створює відчуття захищеності. Що має позитивно впливати на імідж компанії.

Також не менш важливим є встановлення систем сигналізації охоронної та пожежної. Охоронної для додаткового захисту, пожежної згідно із законодавством. Завдяки цим системам підприємство отримує додатковий захист

від несанкціонованого доступу, якщо із системою керування доступом виникнуть якісь перебої, або вона раптом не спрацює належним чином, чи злочинець зможе її обійти. Система охоронної сигналізації виявить спробу проникнення після завершення робочого часу. Також додатковою перевагою охоронної сигналізації є в тому що, якщо буде спроба проникнення то надійде сигнал на пульт охорони або відповідальних осіб від підприємства, що дозволить швидше зреагувати на проникнення та мінімізувати можливі збитки.

Для унеможливлення доступу до відеоархівів і завдяки можливостям камер і відеореєстратора в компанії передбачено хмарний доступ до архіву. Оскільки були використані сучасні IP-камери та мережевий відеореєстратор, то наявність спеціалізованого робочого місця для працівника відеоспостереження не є обов'язковим. Використання хмарних технологій дає можливість доступу до відео з будь-якої точки із можливістю доступу до інтернету. Також використання хмарних технологій обумовлено зручністю.

## **2.4 Функціонування системи**

Функціонування системи охорони базується на чітко визначених принципах і технологіях, які забезпечують її ефективність і надійність. Система складається з трьох основних компонентів та пожежної системи.

Вся система включає в себе 4 підсистеми, основною частиною кожної з цих систем є :

- датчики та сенсори;
- сигнальні пристрої;
- контролери;
- відеоспостереження.

Детальний розгляд функціонування системи дозволив оцінити ефективність, виявити потенційно слабкі місця та запровадити шляхи оптимізації для

забезпечення максимального рівня безпеки для підприємства. Охоронна система ТОВ «Мікрофінанс і компанія» функціонує за наступним алгоритмом.

Відеоспостереження має такий алгоритм роботи. Камери починають безперервний запис відео згідно із своїми налаштуваннями, сигнал з камер поступає до відеореєстратора, який обробляє цей сигнал та стискає його для зберігання на жорсткому диску, відео зберігаються у вигляді файлів на жорсткому диску. В оператора відеонагляду є можливість вибору і перегляду відео в реальному часі, та доступу до відеоархіву.

Блок-схема алгоритму роботи підсистеми відеоспостереження показано на рис. 2.6.

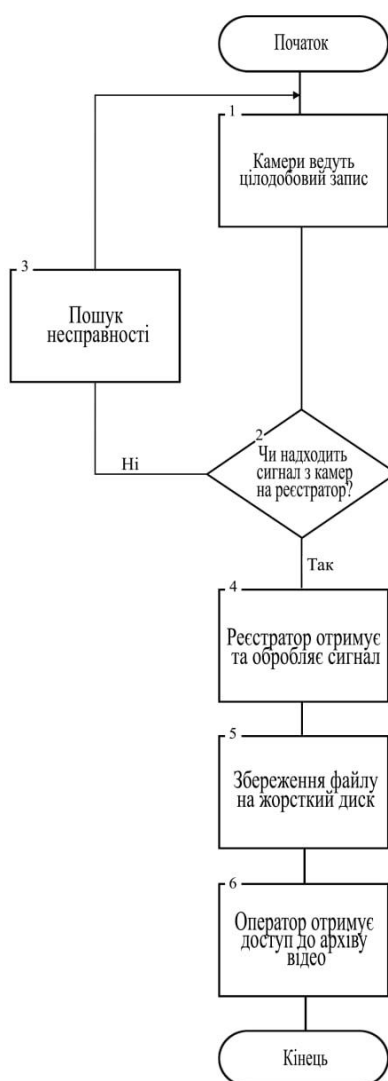


Рисунок 2.6 – Узагальнена блок-схема алгоритму роботи відеоспостереження

Система контролю та управління доступом працює за наступним алгоритмом: користувач підносить картку до зчитувача, вводить пін-код, або проходить біометричну перевірку. Йде передача даних від ідентифікатора на контролер для подальшої обробки. Далі йде швидкий процес авторизації, контролер звіряє отримані дані із базою даних працівників, у разі якщо дані не співпадають у доступі до приміщення буде заборонено. Дані про події дозволу або заборони передаються на центральний пульт для реєстрації та зберігання даних, для подальшого звіту. Оператор або відповідальна людина має можливість дистанційного керування замками, тож він в ручному режимі може надавати або забороняти доступ.

Охоронна сигналізація – датчики руху, відкриття або розбивання скла фіксують подію та передають сигнал на контрольну панель, яка в свою чергу обробляє сигнал та активує звукову сирену та світлові сповіщувачі, далі сигнал тривоги подають на пульт охорони або відповідальної особи.

Користувач активує систему через пульт керування і система переходить у режим охорони, під час активації охоронної система, система надає певний час для користувача якщо виникає якась затримка на виході без надсилання сповіщення на пункт охорони. Датчики постійно мониторять стан об'єкта, передача даних від датчиків відбувається постійно, якщо датчики фіксують якусь дивну подію контролер активує

Пожежна сигналізація є критично важливим елементом забезпечення безпеки будь-яких об'єктів. Її алгоритм роботи є наступним (рис. 2.7) – димові або теплові датчики цілодобово мониторять стан об'єкта для виявлення задимлення або підвищення температури, передають сигнал на контролер, який аналізує дані для виявлення пожежі або інших аномальних ситуацій. При появі ознак пожежі контролер активує систему оповіщення та визначає тип загрози і місце пожежі в цей час також активуються всі світлові і звукові сигнали для оповіщення про загрозу, повідомлення про пожежу отримують екстерні служби.

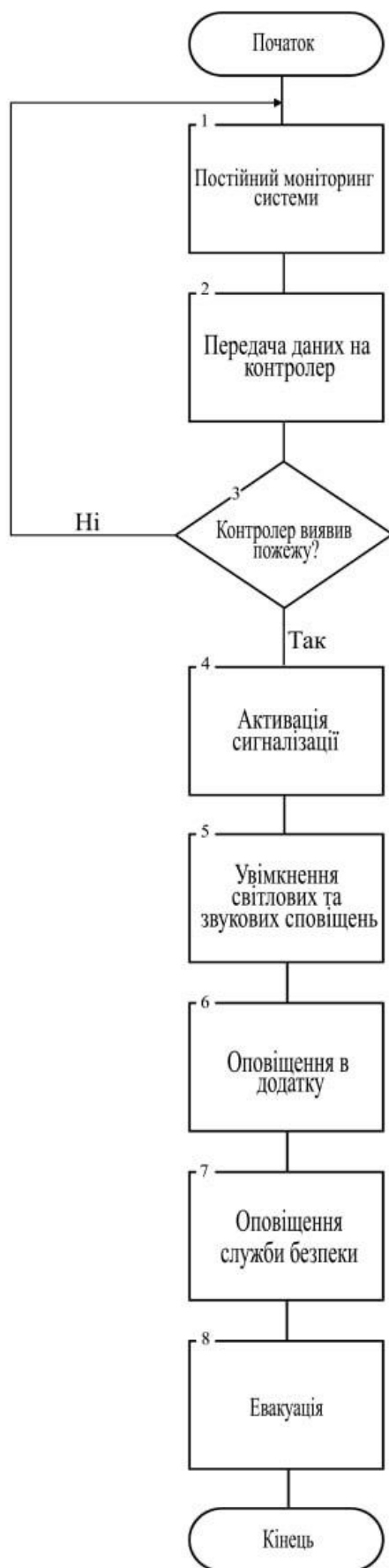


Рисунок 2.7 – алгоритм роботи сигналізації

### **3 АПАРАТНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**

#### **3.1 Вибір апаратного забезпечення системи**

Вибір апаратного забезпечення для охоронної системи є найголовнішим етапом у розробці будь-якої системи безпеки. Це допоможе визначити надійність, ефективність та функціонування системи в загалом. При виборі обладнання необхідно було враховувати такі фактори:

- технічні характеристики;
- надійність та довговічність;
- вартість;
- можливість масштабування.

Технічні характеристики – чутливість датчиків, роздільна здатність камер, пропускна здатність мережевого обладнання, ємність відеореєстратора, тощо.

Надійність та довговічність – обладнання має бути надійним та якісним, здатним працювати в умовах підвищеного навантаження.

Вартість – бюджет на придбання є важливим обмеженням, тому необхідно знайти оптимальне співвідношення ціни та якості.

Можливість масштабування – система має бути спроектована з урахуванням можливості в подальшому її модернізації.

Із урахуванням усіх вище наведених факторів, було прийнято рішення про те що вибір конкретних моделей обладнання буде здійснюватися із урахуванням таких факторів:

- камери – роздільна здатність камери повинна бути Full HD або вище, камера повинна мати ІЧ-підсвічування, широкий кут огляду, ступінь захисту від зовнішніх впливів IP66 або вище;

- відеореєстратор – кількість каналів повинна бути не менше 16, підтримка високої роздільної здатності, достатній обсяг жорсткого диску для нього, вибір жорсткого диску потрібно робити з урахуванням що на ньому якийсь період час убуде зберігатись відеоархів;

- система контролю та управління доступу – тип ідентифікації (карткова або біометрія), кількість точок доступу, можливість інтеграції з різними системами;
- сигналізація – тип датчиків (відкриття дверей та вікон, датчики руху, розбиття скла, диму , тепла), гучність сирен, можливість відправки сповіщень.

На основі аналізу та з урахуванням усіх факторів було обрано наступне обладнання.

Dahua DH-IPC-HFW2431SP-S-S2 (рис 3.1) – купольна IP-камера з роздільною здатністю 4Мп. Має ІЧ-підсвічування до 30 метрів, моторизованим об'єктивом 2.7-13.5мм та ступенем захисту IP67.



Рисунок 3.1 – камера Dahua DH-IPC-HFW2431SP-S-S2

Hikvision DS-7616NI-K2/16P (рис. 3.2) – 16-канальний NVR з підтримкою роздільної здатності до 8 Мп, можливістю встановлення 2х жорстких дисків до 10Тб кожний, та з функціями інтелектуального аналізу відео.



Рисунок 3.2 - Hikvision DS-7616NI-K2/16P

Комплект системи контролю та управління доступом на базі Hikvision DS-K2804 (рис. 3.3) – комплект включає в себе мережевий контролер доступу для 4-х дверей Hikvision DS-K2804, PRIF зчитувачі карток EM-Marine Hikvision DS-K1802E, кнопки виходу ART-801A, безконтактні картки доступу Proximity Card EM-06 (10шт, але така система СКУД включає в себе можливість докупити картки окремо, бо система може включати в себе до 10000 користувачів), магнітні датчики відкриття HO-03K



Рисунок 3.3 – СКУД на базі Hikvision

Комплект пожежної сигналізації та охоронної AJAX STARTERKIT (рис 3.4) до його складу входять – центральний блок Ajax Hub 1 шт, датчики руху Ajax MotionProtect 1 шт, датчики відкриття Ajax DoorProtect strong 1 шт, брелок та два акумулятори, за потребою можливо докупити окремо потрібні датчики, оскільки система може включати в себе до 100 датчиків та вони легко під'єднуються в систему завдяки QR-кодам.



Рисунок 3.4 - AJAX STARTERKIT

### 3.2 Вибір програмного забезпечення

Правильний вибір програмного забезпечення гарантує ефективне управління всіма компонентами, високу надійність та функціональність. Вибір програмного забезпечення для охоронних систем є одним із ключових етапів розробки та впровадження комплексних рішень безпеки. Програмне забезпечення повинно відповідати функціональним вимогам, що висуваються до системи

охорони, якщо вся система інтегрована або сумісні то програмне забезпечення повинно підтримувати різні типи датчиків, контроль доступу. ПЗ має бути надійним, безпечним, мати високу швидкість обробки даних.

Однак все ще лишились критерії такі як зручний та інтуїтивно зрозумілий інтерфейс що полегшить управління та моніторинг системи, забезпечення високого рівня безпеки даних. Програмне забезпечення повинно відповідати функціональним та нефункціональним вимогам, що висуваються до системи охорони. Таким як підтримка обробки сигналів від різних типів датчиків, швидкість обробки даних, продуктивність, надійність, масштабованість, безпека. Програмне забезпечення повинно бути сумісним із компонентами системи та технологіями які були використані. Також програмне забезпечення повинно мати можливість масштабування для подальшого розширення системи без значних змін у структурі. Це важливо для гнучкості та можливості адаптації до зростаючих потреб безпеки. Не менш важливим є наявність якісної технічної підтримки та регулярних оновлень програмного забезпечення. Програмне забезпечення є важливим критерієм для забезпечення безперебійної роботи охоронної системи, це означає що в разі виникнення проблем буде надано оперативну технічну підтримку та регулярні оновлення для покращення функціональності програмного забезпечення.

Існує три типи програмного забезпечення:

- фірмове програмне забезпечення;
- універсальне програмне забезпечення;
- хмарні сервіси.

Фірмове програмне забезпечення - це програмне забезпечення яке було розроблене виробниками обладнання для конкретних моделей, зазвичай воно має обмежену функціональність але є найбільш сумісним із обладнанням.

Універсальне програмне забезпечення – таке програмне забезпечення підтримує обладнання різних виробників та має широкий спектр функцій.

Хмарні сервіси – надають доступ до обладнання через інтернет, це зручний та масштабований варіант але вимагає стабільного інтернет-з'єднання.

Для камер Dahua DH-IPC-HFW2431SP-S-S2 та відеореєстратора Hikvision DS-7616NI-K2/16P та системи контролю та управління доступом було використано фірмове програмне забезпечення Hikvision iVMS-4200 (рис 3.5). Це програмне забезпечення для перегляду та керування IP-камерами, мережевими відеореєстраторами та системами контролю доступу. Є можливість відображати на одному моніторі до 64-х камер з різних відеореєстраторів. Є можливість перегляду архіву записів. Це програмне забезпечення є кросплатформним, оскільки він сумісний з операційними системами Windows, Mac OS, Linux.

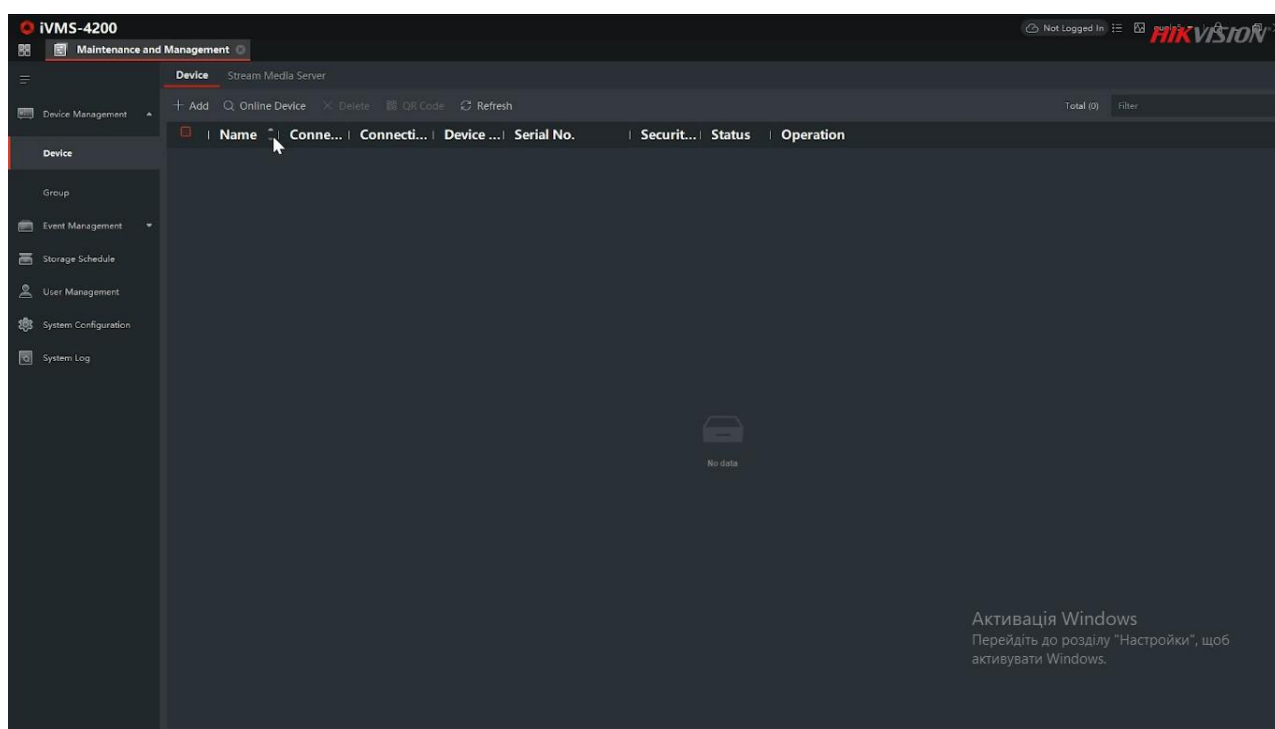


Рисунок 3.5 – інтерфейс програмного забезпечення Hikvision iVMS-4200

Для охоронної та пожежної сигналізації використовується мобільний додаток Ajax Security System (рис 3.6) від виробника, який дозволяє керувати системою, отримувати сповіщення про тривогу та переглядати історію подій. Додаток простий і зрозумілий. Сповіщення надають усю важливу інформацію, що і де сталося, за потреби можна переглянути весь журнал подій. Функція «геозони» дає змогу налаштувати нагадування про встановлення та зняття системи безпеки з охорони. Ajax Security System так само як і Hikvision iVMS-4200 є кросплатформним додатком оскільки є доступним як для Android так і для iOS.

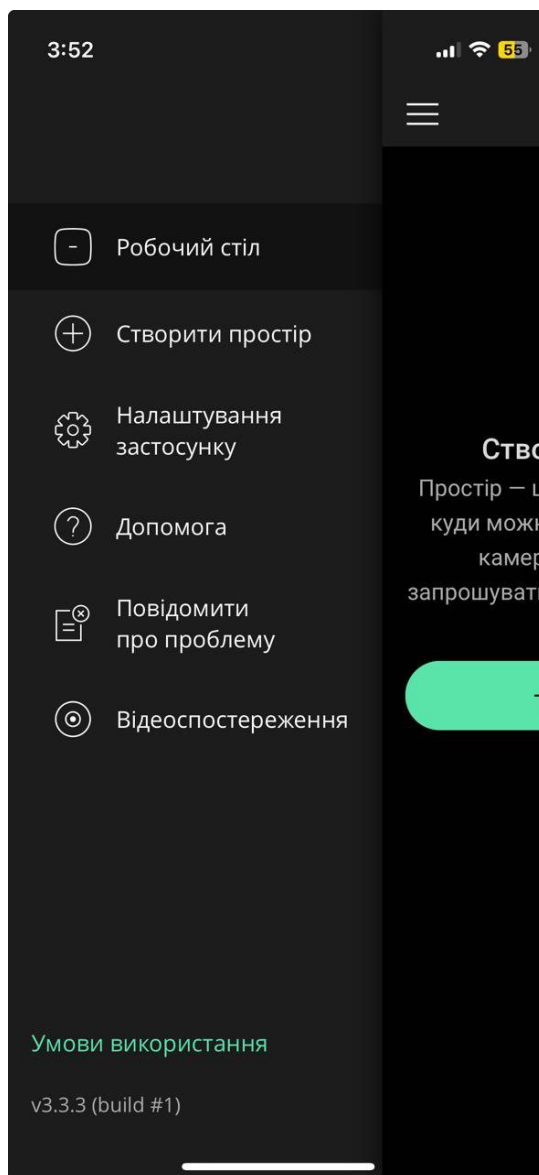


Рисунок 3.6 – Інтерфейс програмного забезпечення Ajax Security System

Також не менш важливим за вибір програмного забезпечення є частина вибору операційної системи, оскільки ОС є основою для роботи програмного забезпечення, за допомогою якого і будуть керувати охоронною системою. Вибір операційної системи впливає на стабільність роботи. Враховуючи специфіку роботи компанії ТОВ «Мікрофінанс і компанія», рекомендовано було використовувати операційну систему з високим рівнем захисту. Було обрано використовувати Windows 10 Pro оскільки вона є популярною системою з широким спектром функцій безпеки, таких як BitLocker. Має можливість налаштування групових політик для обмеження доступу системи. А також це

найпоширеніша операційна система, відома своєю універсальністю, широким вибором програмного забезпечення та простотою використання, Windows має найбільшу бібліотеку програмного забезпечення серед усіх операційних систем, включаючи як популярні програми для роботи та розваг. Так і спеціалізовані програми для різних галузей. Windows сумісна з більшістю комп'ютерів та ноутбуків тож, це означає що не потрібно буде перейматись пошуком потрібних драйверів для встановлення та вирішення проблем сумісності.

#### **4 НАЛАШТУВАННЯ РОБОТИ СИСТЕМИ**

На окремому комп'ютері вже було встановлено Windows Server 2016. Компанія обрала цю серверну ОС через ряд переваг для підключення по RDP. Windows Server 2016 підходить для різних сценаріїв використання, має широкий спектр функцій та покращень у порівнянні із попередніми версіями. Ця версія Windows має 3 варіанти видання:

- Windows Server 2016 Essentials;
- Windows Server 2016 Standard;
- Windows Server 2016 Datacenter.

Windows Server 2016 Essentials – підходить для малого бізнесу (до 25 користувачів та до 50 пристроїв);

Windows Server 2016 Standard – для фізичних або мінімально віртуалізованих середовищ;

Windows Server 2016 Datacenter – для високо віртуалізованих середовищ та хмарних інфраструктур.

Оскільки на підприємстві для захисту конфіденційних даних використовують RDP підключення, було прийнято рішення про створення окремої «відео хмари». Доступ до донної хмари будуть мати декілька людей: працівники служби безпеки офісу, фахівець з відеонагляду, провідні

адміністратори та керівник технічної підтримки. Цей доступ буде надано через обліковий запис в Active Directory.

Переваги використання хмарного доступу до сервісу відео:

- RDP дозволяє налаштувати різні рівні доступу для різних співробітників, що забезпечує безпеку конфіденційних даних;
- економія на обладнанні, через те що немає необхідності купувати потужні робочі машини для окремих співробітників чия робота пов'язано із системою відеонагляду;
- легке розширення RDP-інфраструктури, додаючи нові сервери та користувачів по мірі зростання потреб підприємства.

Active Directory – LDAP- сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows. Active Directory дозволяє адміністраторам системи використовувати групові політики, забезпечує управління об'єктами в мережі таким к користувачі та комп'ютери, групи та інші ресурси. Використання Active Directory надає підприємствам ряд переваг:

- централізоване управління;
- спрощена автентифікація;
- політики безпеки.

Централізоване управління - дозволяє адміністраторам керувати всіма об'єктами мережі з одного місця;

Спрощена автентифікація – за допомогою Active Directory користувачі можуть використовувати єдиний набір облікових даних для доступу до всіх відкритих для них ресурсів;

Політики безпеки – AD дозволяє застосовувати політики безпеки для всіх об'єктів мережі, що забезпечує захист даних та ресурсів.

Remote Desktop Services – це технологія Microsoft, яка дозволяє створювати на керувати інфраструктурою віртуальних робочих столів та віддалених додатків. Вона надає користувачам можливість отримувати доступ до своїх робочих середовищ з будь-якого пристрою із підключеним інтернетом.

Основні компоненти Remote Desktop Services:

- remote desktop connection broker;
- remote desktop session host;
- remote desktop web access;
- remote desktop gateway;
- remote desktop licensing.

Remote desktop connection broker - відповідає за перенаправлення користувачів на робочі столи які для них доступні;

Remote desktop session host - це сервер, на якому розміщуються сеанси віддалених робочих столів та додатків;

Remote desktop web access - надає користувачам інтерфейс для доступу до робочих столів та додатків;

Remote desktop gateway - забезпечує безпечний доступ до ресурсів;

Remote desktop licensing - керує ліцензіями на доступ до Remote Desktop Services.

За допомогою всіх вище перерахованих компонентів, було створено окремий віддалений робочий стіл куди встановили програмне забезпечення для керування системою відеонагляду та системою керування та управління доступом. Відповідним людям надали доступ до даної хмари із обліковими доменними даними.

Для встановлення необхідного програмного забезпечення необхідно було перейти на сайт виробника, та завантажити з веб-ресурсу програму. Після встановлення при першому вході в програму пропонується створення облікового запису адміністратора, де потрібно ввести логін та пароль. На вкладці «керування пристроями» через клавішу «додати» обираємо тип пристрою який будемо додавати, його IP-адресу та порт на який він підключений, також необхідно додати ім'я користувача. На вкладці «основний перегляд» можна вибрати пристрої які необхідно переглядати. Також можна налаштувати макет відображення, вибравши кількість вікон які будуть відображатись. В розділі «сервер зберігання» можна налаштувати параметри запису: пристрої з яких буде

йти запис, розклад запису та його тривалість.

Систему керування та управління доступом додаємо так само як і камери, через вкладку керування пристроями та додати. На вкладці «контроль доступу» можна налаштувати двері, зони доступу, розклади, рівні доступу та інші параметри згідно з потребами підприємства. Далі необхідно створити облікові записи користувачів та призначити їм відповідні рівні доступу.

Також в додатку можна визначити події які будуть викликати сигнал тривоги, та дії охоронної системи на ці події, такі як надсилання повідомлення або запис відео.

Для налаштування пожежної та охоронної системи, необхідно було встановити центральний хаб системи безпеки в безпечному місці, підключити його до живлення та інтернету, розташувати всі необхідні датчики. Наступним кроком після встановлення всіх датчиків та сенсорів необхідно було встановити додаток системи безпеки Ajax Security System. Для створення облікового запису в додатку необхідно було дотримуватись інструкцій. Після входу в обліковий запис в додатку є функція «додати хаб» для того щоб додати хаб в додаток безпеки необхідно було відсканувати QRкод на задній частині хаба. Після того як додали всі елементи системи дотримуючись інструкцій самого додатка можна налаштувати режими охорони. Налаштування режимів – вибір пристроїв які будуть активними в певний період часу. Також в додатку можна вибрати, які дії повинні викликати сповіщення( реагування датчика, або втрата зв'язку з пристроєм). Також можна налаштувати в який спосіб будуть отримуватись сповіщення – це або push- повідомлення або SMS-інформування, або дзвінок.

Наступний крок в налаштуванні охоронної системи є найголовнішим – в додатку буде доступний вибір охоронної фірми, яка співпрацює з обладнанням Ajax. Після вибору охоронної фірми в додатку, компанія ТОВ «Мікрофінанс і компанія» уклала договір з представниками охоронної фірми, для захисту об'єкта. Наступним нашим кроком було надання унікального ідентифікатора хабу Ajax. Охоронна компанія зі свого боку налаштувала своє обладнання для отримання сигналів від нашого хабу. Зі свого боку ми додали в налаштування хабу контакти

охоронної фірми. Після завершення налаштувань, охоронна фірма провела тестування зв'язку з хабом Ajax. Тестування пройшло успішно, в офіс охоронної фірми поступив сигнал про тривогу, повідомлення передали до патрульної служби, яка приїждить на сигнал тривоги, та вона приїхала протягом 20 хвилин.

## ВИСНОВКИ

У даній дипломній роботі було проведено всебічний аналіз і розроблено рекомендації по створенню ефективної системи безпеки для компанії. В ході роботи було проаналізовано новітні технології забезпечення безпеки, що включають в себе системи контролю доступом, відеоспостереження та сигналізації.

Було виявлено, що інтегруючи ці підсистеми в одну велику систему можна досягти вищого рівня безпеки та швидкого реагування на загрози.

Вибір оптимального технічного рішення був зроблений з урахуванням особливостей об'єкта, його розміру, виду діяльності та потенційних загроз. Виходячи з цього було підібрано відповідне обладнання та програмне забезпечення, які забезпечать максимальну ефективність та надійність системи безпеки.

Були розроблені алгоритми для різних компонентів системи безпеки. Ці алгоритми забезпечують чітке і скоординоване функціонування системи, дозволяючи швидко виявляти загрози та реагувати на них.

Також був проведений детальний аналіз ринку програмного забезпечення для системи безпеки. Вибір програмного забезпечення ґрунтувався на сумісності, надійності, захищеності, масштабованості та простоті використання.

Забезпечення безпеки об'єкта – складна і багатогранна задача, що вимагає комплексного підходу та використання новітніх технологій. Проведені дослідження і розроблені рекомендації дозволяють створити ефективну систему безпеки, яка на високому рівні захищає приміщення від різних загроз. Впровадження пропонованого рішення допоможе підвищити рівень безпеки, знизити ризики і захистити майно і персонал компанії.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Класифікація камер спостереження. URL: [https://kristall-systems.net.ua/ua/novosti/classification\\_of\\_cameras\\_for\\_video\\_surveillance/](https://kristall-systems.net.ua/ua/novosti/classification_of_cameras_for_video_surveillance/) (дата звернення 30.03.2024)
2. Види камер відеоспостереження. URL: <https://www.gazik.com.ua/vydy-kamer-videosposterezhennya.html> (дата звернення 31.03.2024)
3. Типи відеореєстраторів для систем відеоспостереження. URL: <https://pipl.ua/article/tipi-videoreyestratoriv-dlya-sistem-videosposterejennya> (дата звернення 02.04.2024)
4. Системи контролю доступу – що це і як працює. URL: <https://ssbb.ua/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/sistemy-ontrolya-dostupa-cho-eto-i-kak-eto-rabotaet/> (дата звернення 05.04.2024)
5. Що таке скуд? URL: <https://ssbb.ua/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/sho-takoe-skud/> (дата звернення 07.04.2024)
6. Кілька кроків, щоб ефективно захистити свою компанію від злодіїв. URL: <https://access.dp.ua/kilka-kroktiv-shob-efektivno-zahistiti-svoyu-kompaniyu-vid-zlodiiv/> (дата звернення 10.04.2024)
7. З чого складається система пожежної сигналізації? URL: <https://worldvision.com.ua/iz-chego-sostoit-sistema-pozharnoy-signalizatsii/> (дата звернення 12.04.2024)
8. Охоронна сигналізація. URL: <https://www.arsenal-st.com.ua/ohoronna-signalizaciya/> (дата звернення 13.04.2024)
9. ТОВ «Фаєр-контроль». URL: <https://tovfirecontrol.wordpress.com> (дата звернення 15.04.2024)
10. Система безпеки підприємства. URL: <http://surl.li/udmyh> (дата звернення 15.04.2024)
11. що таке система безпеки та як вона працює? URL: <https://dneprsecurity.com/statji/cho-takoe-sistema-bezopasnosti-i-kak-ona->

rabotaet.html (дата звернення 17.04.2024)

12. Взаємодія бездротової Ajax з дротовими системами сигналізації. URL: <https://dneprsecurity.com/statji/besprovodnaja-ajax-s-provodnimi-sistemami.html> (дата звернення 20.04.2024)

13. Контроль доступу – ключ до ефективного використання простору. URL: <https://dneprsecurity.com/statji/kontrol-dostupa---kljuch-k-jeffektivnomu-ispolzovaniju-prostranstva.html> (дата звернення 23.04.2024)

14. Популярні категорії. URL: <https://hikvision.co.ua/> (дата звернення 27.04.2024)

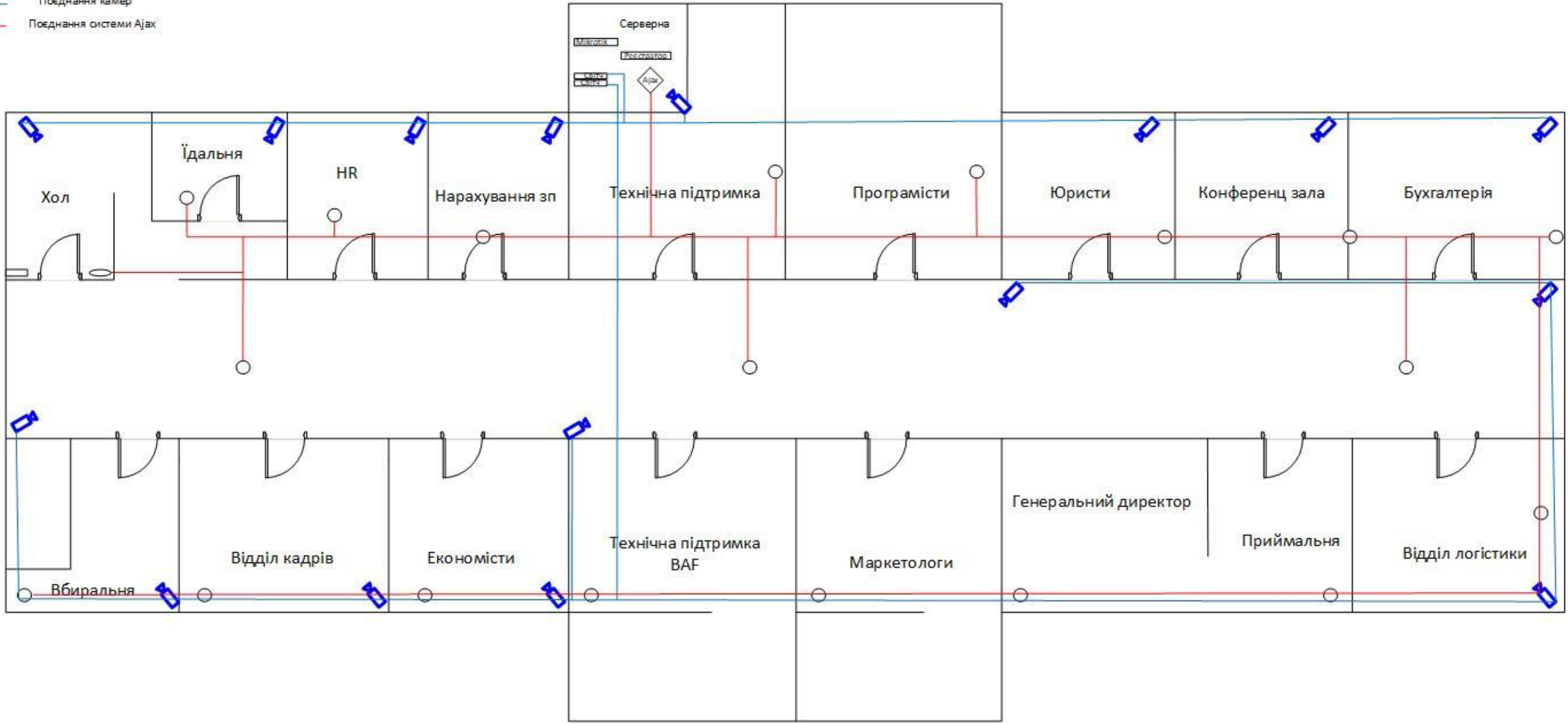
15. Новинки. URL: <http://surl.li/udnbo> (дата звернення 02.05.2024)

16. Встановлення доменних служб Active Directory в Керуванні сервером. URL: [ntrosv.com.ua/docs/vstanovlennya-active-directory-domain-services-u-server-manager/](https://ntrosv.com.ua/docs/vstanovlennya-active-directory-domain-services-u-server-manager/) (дата звернення 10.05.2024)

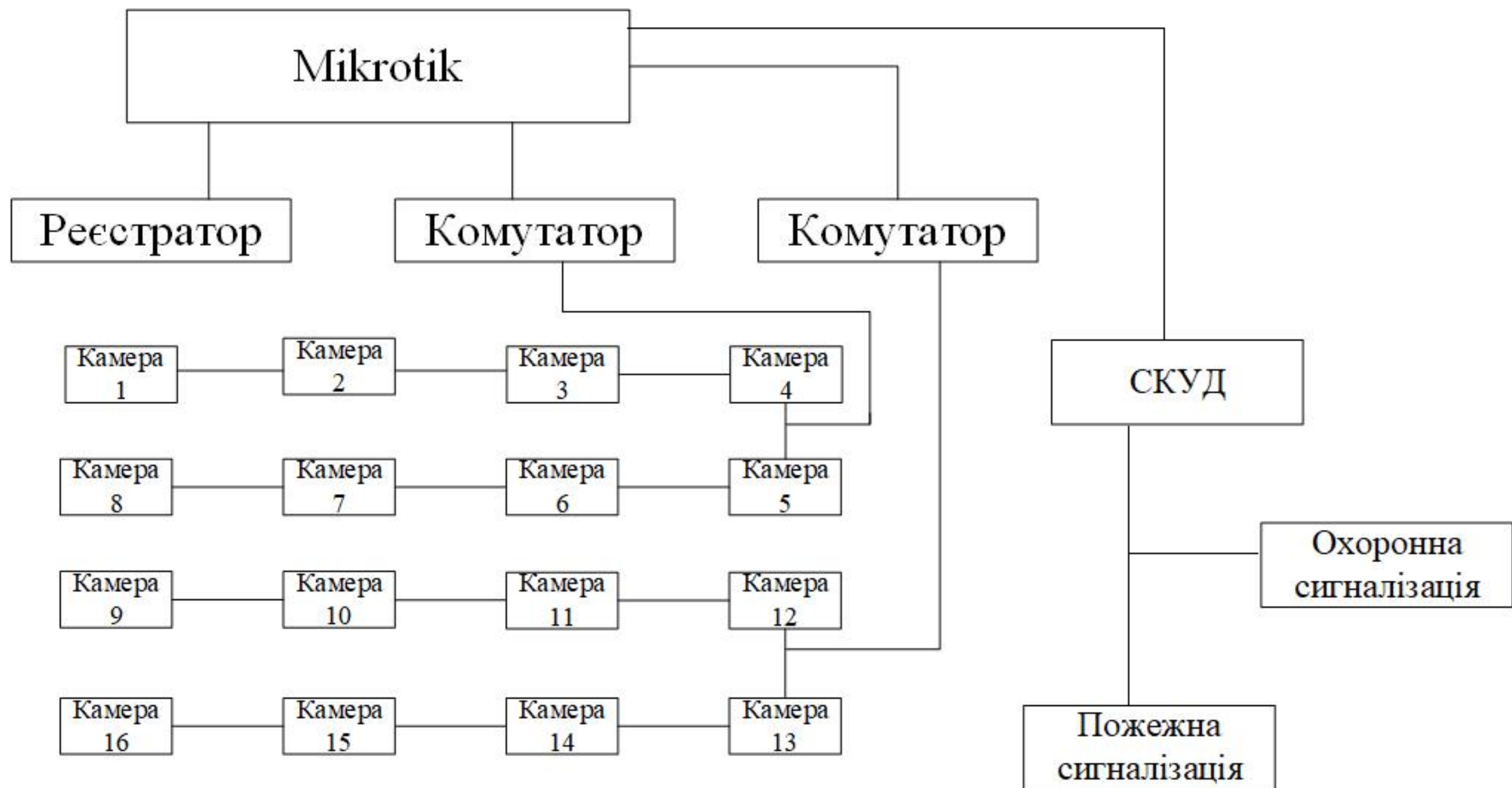
17. Налаштування RDP на Windows Server. URL: <https://cherkasy.lvivservice.com.ua/nalashtuvannya-rdp-na-windows-server> (дата звернення 15.05.2024)

18. Керуй своїм простором. URL: <https://ajax.systems.ua/> (дата звернення 20.05.2024)

- СКУД
- Датчик відкриття дверей
- Датчик вогню та диму
- Поеднання камер
- Поеднання системи Аїах



|           |      |                |                                                                                       |      |                           |                                       |  |          |         |  |  |
|-----------|------|----------------|---------------------------------------------------------------------------------------|------|---------------------------|---------------------------------------|--|----------|---------|--|--|
|           |      |                |                                                                                       |      | 13.02070849.51120 ПЛ1     |                                       |  |          |         |  |  |
|           |      |                |                                                                                       |      | Монтажна схема приміщення | Літ.                                  |  | Маса     | Масштаб |  |  |
| Зм        | Лист | № докум.       | Підп.                                                                                 | Дата |                           |                                       |  |          |         |  |  |
| Розроб.   |      | Дрозда К.А     |  |      |                           |                                       |  |          |         |  |  |
| Перевір.  |      | Тягунова М.Ю   |  |      |                           |                                       |  |          |         |  |  |
| Т. контр. |      |                |                                                                                       |      |                           |                                       |  |          |         |  |  |
|           |      |                |                                                                                       |      |                           | Лист. 1                               |  | Листів 1 |         |  |  |
| Н. контр. |      | Щербак Н.В.    |  |      |                           | НУ «Запорізька політехніка» КНТ-511сп |  |          |         |  |  |
| Затв.     |      | Кудерметов Р.К |  |      |                           |                                       |  |          |         |  |  |



|           |                 |          |                                                                                       |      |                                |                                       |          |         |  |
|-----------|-----------------|----------|---------------------------------------------------------------------------------------|------|--------------------------------|---------------------------------------|----------|---------|--|
|           |                 |          |                                                                                       |      | 13.02070849.51120 ПЛ2          |                                       |          |         |  |
|           |                 |          |                                                                                       |      | Структурна схема роботи истеми | Літ.                                  | Маса     | Масштаб |  |
| Зм        | Лист            | № докум. | Підп.                                                                                 | Дата |                                |                                       |          |         |  |
| Розроб.   | Дрозда К.А.     |          |  |      |                                |                                       |          |         |  |
| Перевір.  | Тягунова М.Ю.   |          |  |      |                                |                                       |          |         |  |
| Т. контр. |                 |          |                                                                                       |      |                                |                                       |          |         |  |
|           |                 |          |                                                                                       |      |                                | Лист. 1                               | Листів 1 |         |  |
| Н. контр. | Щербак Н.В.     |          |  |      |                                | НУ «Запорізька політехніка» КНТ-511сп |          |         |  |
| Затв.     | Кудерметов Р.К. |          |  |      |                                |                                       |          |         |  |



Камера Dahua



Реєстратор Hikvision



Сигналізація Ајах

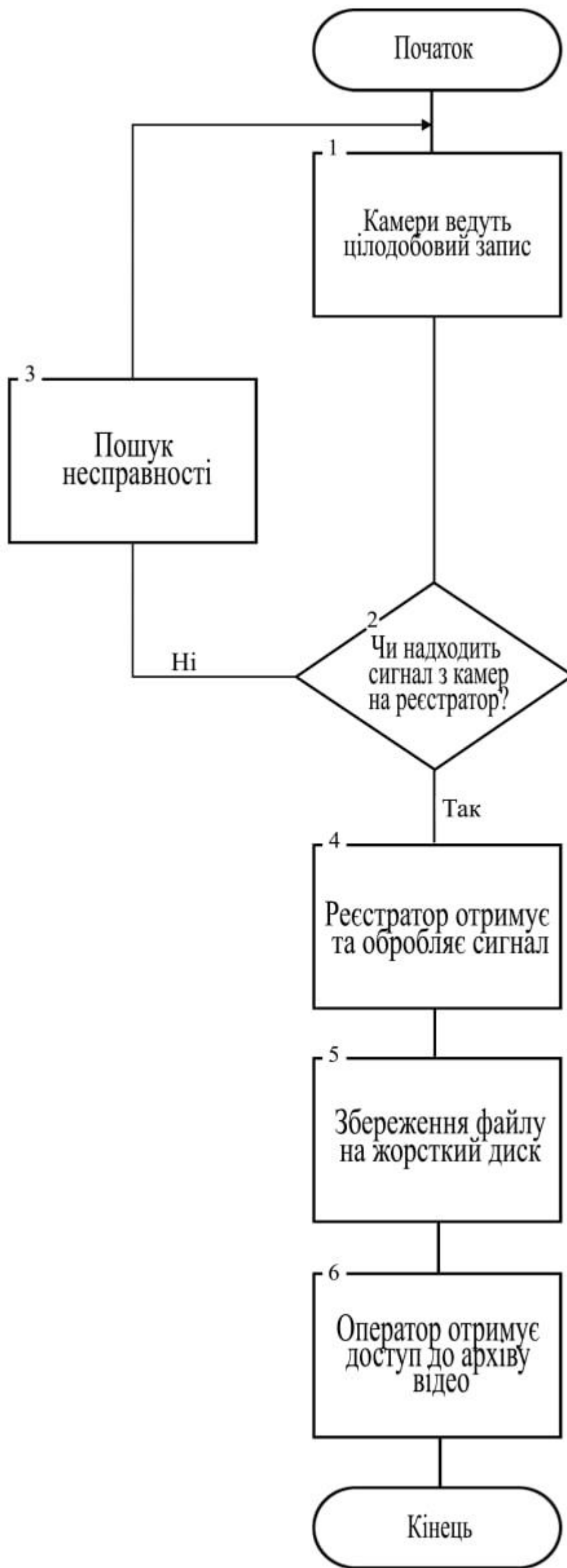


СКУД на базі Hikvision

|           |                 |          |       |      |                                            |                                       |  |  |          |         |  |
|-----------|-----------------|----------|-------|------|--------------------------------------------|---------------------------------------|--|--|----------|---------|--|
|           |                 |          |       |      | 13.02070849.51120 ПЛЗ                      |                                       |  |  |          |         |  |
|           |                 |          |       |      | Зображення апаратного забезпечення системи | Літ.                                  |  |  | Маса     | Масштаб |  |
| Зм        | Лист            | № докум. | Підп. | Дата |                                            |                                       |  |  |          |         |  |
| Розроб.   | Дрозда К.А.     | Е.А.     |       |      |                                            |                                       |  |  |          |         |  |
| Перевір.  | Тягунова М.Ю.   | М.Ю.     |       |      |                                            |                                       |  |  |          |         |  |
| Т. контр. |                 |          |       |      |                                            |                                       |  |  |          |         |  |
|           |                 |          |       |      |                                            | Лист. 1                               |  |  | Листів 1 |         |  |
| Н. контр. | Щербак Н.В.     | Н.В.     |       |      |                                            | НУ «Запорізька політехніка» КНТ-511сп |  |  |          |         |  |
| Затв.     | Кудерметов Р.К. | Р.К.     |       |      |                                            |                                       |  |  |          |         |  |



|           |      |                 |                                                                                      |      |                                              |                                       |  |          |         |  |  |
|-----------|------|-----------------|--------------------------------------------------------------------------------------|------|----------------------------------------------|---------------------------------------|--|----------|---------|--|--|
|           |      |                 |                                                                                      |      | 13.02070849.51120 A1                         |                                       |  |          |         |  |  |
|           |      |                 |                                                                                      |      | Блок-схема алгоритму роботи підсистеми відео | Літ.                                  |  | Маса     | Масштаб |  |  |
| Зм        | Лист | № докум.        | Підп.                                                                                | Дата |                                              |                                       |  |          |         |  |  |
| Розроб.   |      | Дрозда КА       |  |      |                                              |                                       |  |          |         |  |  |
| Перевір.  |      | Тягунова М.Ю    |  |      |                                              |                                       |  |          |         |  |  |
| Т. контр. |      |                 |                                                                                      |      |                                              |                                       |  |          |         |  |  |
|           |      |                 |                                                                                      |      |                                              | Лист. 1                               |  | Листів 1 |         |  |  |
| Н. контр. |      | Щербак Н.В.     |  |      |                                              | НУ «Запорізька політехніка» КНТ-511сп |  |          |         |  |  |
| Затв.     |      | Кудерметов Р.К. |  |      |                                              |                                       |  |          |         |  |  |



|           |      |                 |                                                                                      |      |                                              |                                       |  |          |         |  |  |
|-----------|------|-----------------|--------------------------------------------------------------------------------------|------|----------------------------------------------|---------------------------------------|--|----------|---------|--|--|
|           |      |                 |                                                                                      |      | 13.02070849.51120 A1                         |                                       |  |          |         |  |  |
|           |      |                 |                                                                                      |      | Блок-схема алгоритму роботи підсистеми відео | Літ.                                  |  | Маса     | Масштаб |  |  |
| Зм        | Лист | № докум.        | Підп.                                                                                | Дата |                                              |                                       |  |          |         |  |  |
| Розроб.   |      | Дрозда К.А      |  |      |                                              |                                       |  |          |         |  |  |
| Перевір.  |      | Тягунова М.Ю    |  |      |                                              |                                       |  |          |         |  |  |
| Т. контр. |      |                 |                                                                                      |      |                                              |                                       |  |          |         |  |  |
|           |      |                 |                                                                                      |      |                                              | Лист. 1                               |  | Листів 1 |         |  |  |
| Н. контр. |      | Щербак Н.В.     |  |      |                                              | НУ «Запорізька політехніка» КНТ-511сп |  |          |         |  |  |
| Затв.     |      | Кудерметов Р.К. |  |      |                                              |                                       |  |          |         |  |  |

