Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему **МОДЕРНІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ТА КОНТРОЛЮ ДОСТУПУ З ІНТЕГРАЦІЄЮ У ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ ТОВ «ІНДУСТРІАЛЬНІ СИСТЕМИ АВТОМАТИЗАЦІЇ»**

Виконав: студент 6 курсу, групи 601ТТ
спеціальності 172 «Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Плутцов Є.М.
(прізвище та ініціали)
Керівник Шефер О.В
(прізвище та ініціали)
Рецензент Кислиця С.Г.
(прізвище та ініціали)

Полтава - 2022 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Магістр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій

_____ О.В. Шефер
“___” _____ 2022 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Плутцову Євгенію Миколайовичу

1. Тема проекту (роботи) **«Модернізація системи безпеки та контролю доступу з інтеграцією у телекомунікаційну мережу ТОВ «Індустріальні Системи Автоматизації»**
керівник проекту (роботи) Шефер Олександр Володимирович, д.т.н., доцент
затверджена наказом вищого навчального закладу від “12 ” 08 2022 року № 544 фа

2. Строк подання студентом проекту (роботи) 07.12.2022 р.

3. Вихідні дані до проекту (роботи) мережа ТОВ «Індустріальні Системи Автоматизації», мережеве обладнання

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вибір необхідного обладнання при побудові системи безпеки для підприємства. Організація контролю доступу.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
1) Схема зон контролю доступу
2) Схема визначених об’єктів охорони
3) Обладнання для системи охорони безпеки
4) Схема точок монтажу контролеру
5) Схема інтеграції контролеру до мережі підприємства
6) Схема встановлення оповіщення та протипожежної безпеки
7) Місцерозташування обладнання відеоспостереження
8) Схема монтажу кінцевого обладнання

6. Дата видачі завдання 01.09.2022 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Примітка (плакати)
1	Огляд сучасних протоколів передачі даних у система безпеки	13.09.22		15%	Пл. 1
2	Принципи комплексного забезпечення безпеки та контролю на підприємстві	27.09.22	I	30%	Пл. 2
3	Визначення проєкту системи безпеки	10.10.22		40%	Пл. 4
4	Опис проєкту системи безпеки	17.10.22		50 %	Пл. 5
5	Аналіз та вибір засобів та обладнання для системи безпеки	25.10.22	II	60%	Пл.6,7
6	Впровадження системи безпеки із контролем доступу на підприємстві	07.11.22		70%	Пл.8
7	Оформлення магістерської роботи	07.12.22	III	100%	

Магістрант _____ Плутцов Є.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Шефер О.В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

PoE – технологія живлення через Ethernet кабель

DVR – аналоговий відео-реєстратор

NVR – мережевий відео-реєстратор

LAN – локальна мережа

WAN – глобальна мережа

БД – база даних

NAS – файлове сховище

ВСТУП

Організація безпеки підприємства — це цілісна та багатогранна концепція, спрямована на виявлення, запобігання бізнес-ризиків. До них належать зовнішні загрози, помилкові порушення правил співробітниками та ризики інших сторін. Дані клієнтів та компанії є вразливими, і їх захист є головним пріоритетом будь-якого підприємства [1].

Інформаційна безпека підприємства – це захист цифрових активів та інформації організації. Це може включати будь-що: від веб-сайту організації та онлайн-присутності до її внутрішніх мереж і даних. Щоб захистити ці активи, організації повинні мати комплексну стратегію інформаційної безпеки, яку доповнює фізична безпека.

Фізична безпека підприємства – це захист від фізичного впливу зловмисників чи нещасних випадків. Наприклад фізичне розмежування прав доступу працівників до приміщення чи захист серверів де зберігається конференційні дані клієнтів компанії.

Контроль доступу або керування доступом – ця технологія може релізуватися по різному в залежності від потреб підприємства. Наприклад це може бути видача персоналу смарт-карток, для контролю переміщення та керування доступом до приміщень працівника. Вся інформація про входи та виходи записується у корпоративну базу даних (БД). Така система відносно дешевою та надає реалізацію систему контролю доступу.

Комплексна система захисту підприємства складається із об'єднання декількох систем безпеки – фізичної, інформаційної (кібербезпеки), контролю доступу та пожежної системи безпеки [2].

Пожежна система захисту підприємства – це комплекс технічних засобів призначення яких виявляти факт виникнення пожару та відповідним чином на нього реагувати, розблокуванням дверей, гасінням, викликом аварійних служб [3]. Пожежна система складається із блоку сенсорів – датчиків, контрольно-керуючих панелей, блоків обробки інформації із датчиків – контролерів.

У підприємства ТОВ «Індустріальні Системи Автоматизації» виникла потреба модернізації корпоративної мережі із розширенням її функціоналу до повноцінного комплексного захисту систем безпеки для підприємства. Це підприємство займається обслуговуванням, налаштуванням та інсталяцією інформаційних систем на основі персональних комп'ютерів та систем відео-нагляду. Очевидно що у такого підприємства є потреба захищати свої активи у вигляді обладнання, співробітників, конференційних даних та ділової репутації.

Актуальність даної роботи обумовлюється поширенням нових векторів атак на бізнес у сучасному світі, як фізичним втручанням і інформаційним кібер-атакам на критично важливу бізнес-інфраструктуру. Окрім цього розширення підприємства ТОВ «Індустріальні Системи Автоматизації» обумовлює наявність потреби його захисту та зменшення ризиків від дій зловмисних осіб та аварійних ситуацій із розробкою відповідного проєкту модернізації мережі безпеки із контролем доступу та її інтеграції у мережу підприємства.

Мета роботи – створення проекту модернізації системи безпеки та системи контролю доступу на підприємстві.

Об'єкт дослідження – проект модернізації системи безпеки та системи доступу.

Задачі досліджень даної кваліфікаційної роботи:

- аналіз сучасних системи безпеки на підприємстві;
- огляд сучасних протоколів передачі даних у системах безпеки;
- аналіз та вибір засобів та обладнання для побудови системи безпеки на підприємстві;
- визначення розташування компонентів системи безпеки;
- розрахунок вартості проекту системи безпеки.

1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ СИСТЕМ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

1.1 Актуальність систем безпеки у сучасному світі

Системи безпеки допомагають стримувати зловмисників від проникнення на підприємств, а також постійно захищають фізичні та інформаційні активи. Важливість систем безпеки неможливо переоцінити, але перелічимо основні причини та особливості які надає встановлена система безпеки підприємству [1, 4]:

- Мінімізація можливих втрат – звичайно, сучасні системи безпеки можуть бути досить дорогими, але натомість мають гарне співвідношення ціни та якості, оскільки вони захищають інвестиції та активи підприємства, які коштують набагато дорожче.
- Безпечне середовище для роботи – підприємство несе відповідальність за здоров'я та безпеку своїх працівників. Встановлення систем безпеки сприяє створенню безпечного робочого середовища, забезпечуючи постійний контроль за співробітниками. У разі нещасного випадку чи навмисних злих дій можлива негайна реакція для вирішення проблеми.
- Аналіз отриманих даних – за допомогою різних датчиків та камер можливо створювати аналітичні звіти та автоматизовані системи. Вони представляють дані що можуть покращити використання ресурсів підприємства або полегшити контроль будь-яких надзвичайних ситуацій.
- Встановлені системи безпеки знижують кошторис страхування майна. Оскільки страхові компанії зменшують суму платіжок, коли у підприємства є система безпеки, тому що це призводить до зниження ризику.

Старих методів розгляду інформаційної та фізичної безпеки як окремих сутностей уже недостатньо для захисту підприємства. Однак, зосереджуючись на практиках кіберзахисту, організації часто ігнорують свої потреби у фізичній безпеці. Конвергенція безпеки поєднує стратегії інформаційної та фізичної безпеки, щоб захистити підприємства від нових загроз і вразливостей.

Розглянемо поширені загрози інформаційній та фізичній безпеці підприємства у сучасному світі [4]:

- Зовнішні атаки – вони включають зловмисні спроби сторонніх осіб отримати інформацію, дані або фізичний доступ. Фішинг, соціальна інженерія та злом пристроїв Інтернету речей — усе це приклади загроз безпеці підприємства із зовнішніх джерел. Центри обробки даних більше не є єдиною основною мішенню для хакерів; периферійні пристрої, такі як корпоративні камери безпеки, все частіше стають цілями цих атак.
- Внутрішні атаки – доволі велика кількість інцидентів безпеки підприємства фактично здійснюється співробітниками організації. Такі проблеми, як крадіжка майна, вандалізм, викрадення даних і насильство на робочому місці, є серйозними вразливими місцями безпеки.
- Випадкові порушення безпеки співробітниками. Недостатня політика безпеки, незахищені мережі та застарілі системи безпеки є лише деякими прикладами того, як можуть статися випадкові порушення безпеки. Це може бути наприклад: крадіжки та неправильні облікові дані доступу.

Отже система безпеки є абсолютно необхідною для будь-якого розміру підприємства. Система безпеки окупиться в довгостроковій перспективі підприємству за рахунок зниження витрат у зловмисних, аварійних чи не запланованих ситуаціях.

Рисунок 1.1 – Типові вектори атак для підприємства

1.2 Сучасні протоколи передачі даних у системах безпеки

Бездротові протоколи набувають все більшого розповсюдження у системах безпеки оскільки дозволяють підключати датчики без кабелів, але дротові протоколи також мають свої переваги у вигляді надійності. Перелічимо основні види сучасних протоколів [5,6]:

- Jeweller – це протокол розроблений Ajax Systems для радіозв'язку у системах безпеки. Працює у двох напрямках. Підтримує зміну частоти радіоканалу, дальність до 2км по прямій видимості, захищений блоковим шифруванням. Може бути масштабований використовуючи 5 ретрансляторів та підключити до 200 пристроїв. Цей протокол працює у частотному діапазоні 868,0-868,6 МГц або 868,7-869,2 МГц. Двосторонній зв'язок надає переваги у вигляді економії батареї, під час встановлення режиму очікування на датчиках по команді від центрального хабу. Також енергоефективність досягається за допомогою використання тимчасового розподілу каналів – TDMA.
- KNX RF – це бездротова версія фізичних рівнів KNX. KNX RF може спільно використовувати прикладні рівні з іншими медіаверсіями KNX, тому він повністю сумісний на прикладному рівні. Протокол працює на частоті 868,3 МГц, використовуючи модуляцію FSK зі швидкістю передачі даних 16,4 кбіт/с. KNX RF дозволяє використовувати однонаправлені пристрої (тільки для передачі) на додаток до звичайних двонаправлених пристроїв. Скасувавши функцію приймача, розробник пристрою може продовжити термін служби батареї датчиків підприємства.

  Типовий діапазон прямої видимості KNX RF на частоті 868 МГц становить 150 метрів. Діапазон усередині будівлі дуже залежить від фактичного середовища, будівельних матеріалів тощо. За сприятливих обставин можливий діапазон до 30 метрів у межах будівлі.
- Zigbee – це стандарт IEEE (Інститут інженерів з електротехніки та електроніки) для бездротових домашніх мереж [8]. Це малопотужна, безпечна технологія для Smart House та систем безпеки. Низьке енергоспоживання: ZigBee дозволяє пристроям споживати дуже мало енергії.

Це робить його придатним для використання з пристроями, що живляться від батареї, наприклад камерами безпеки. ZigBee має низьку затримку, що означає, що він може легко передавати високошвидкісні дані (наприклад, зображення та відео). Надійна безпека: ZigBee використовує надійні алгоритми шифрування та автентифікації, які захищають ваші дані від кіберзагроз. Легке встановлення: пристрої ZigBee легко встановити, оскільки вони працюють за допомогою широко доступних шлюзів Wi-Fi або Z-Wave і систем домашньої автоматизації.

- KNX — це система керування, яка була розроблена для бездоганної взаємодії продуктів від різних виробників. Система працює на стандартизованому шинному кабелі, що дозволяє різним продуктам працювати разом. Цей протокол може контролює всі аспекти управління домом і будівлею системи безпеки та дверного зв'язку, аудіо та відео та вимірювання. Протокол KNX використовує одну екрановану пару кабелю для з'єднання всіх пристроїв KNX (перемикачів, приводів тощо) у систему шини. Кожному пристрою в системі надається індивідуальна адреса, що дозволяє іншим пристроям у системі безпечно маршрутизувати та обмінюватися даними з метою керування (увімкнення світла) та зворотного зв'язку (кімнатна температура).

1.3 Принципи комплексного забезпечення безпеки та контролю на підприємстві

1.3.1 Забезпечення фізичної охорони

Заходи фізичної безпеки призначені для захисту будівель і захисту обладнання всередині. Вони не допускають небажаних людей і надають доступ авторизованим особам. Хоча інформаційна безпека також важлива, але запобігання порушенням фізичної безпеки є ключовим для збереження технологій і даних підприємства та будь-якого персоналу, які мають доступ до будівлі. Фізична безпека компанії та її особистих офісів є життєво важливим елементом загальної

безпеки, оскільки вона запобігає втраті життів і власності, а також крадіжці цінного часу, грошей та інформації [1,4].

Є кілька способів встановити фізичну охорону навколо підприємства:

- Переконатися у міцності конструкція дверей та віконними рам, оскільки це перший вектор фізичної атаки підприємства.
- Встановлення охоронної сигналізації, щоб попередження про потенційних зловмисників. Це дозволить фіксувати будь-яку підозрілу діяльність та вжити відповідних заходів.
- Охорона периметру підприємства – паркан із датчиками порушення зон безпеки. Також варто розглянути можливість встановлення якісного охоронного освітлення.

Розглянемо основні аспекти фізичної безпеки підприємству:

- Виявлення – допомагають ідентифікувати потенційну подію безпеки або зловмисника. Датчики, сигнали тривоги й автоматичні сповіщення — усе це приклади виявлення фізичної безпеки.
- Стримування – це фізичні заходи безпеки, які не дають людям виходити з простору. Компонентами безпеки, можуть бути фізичні перешкоди, такі як стіни, двері та вікна. Системи контролю доступу та камери відеоспостереження також запобігають несанкціонованим особам від спроб доступу до будівлі.
- Затримка – є певні системи безпеки, які призначені для уповільнення зловмисників, коли вони намагаються проникнути на об'єкт чи будівлю. Контроль доступу, наприклад, запит на картку-ключ або облікові дані мобільного телефону, є одним із методів затримки.
- Відповідь – реакція на те коли відбувається порушення чи вторгнення. Приклади реагування фізичної безпеки включають системи зв'язку, блокування будівель і звернення до екстрених служб або охоронних служб реагування.

Системи контролю фізичного доступу – дозволяють регулювати та керувати доступ до дверей підприємства. Встановлення системи контролю доступу надає

захист від неконтрольованих точок входу – відкритих дверей, вікон, від несанкціонованого доступу в чутливі зони та неконтрольованого доступу звичайних відвідувачів. Нижче наведено список функцій, які повинна виконувати система контролю фізичного доступу [4].

- Обмеження доступу – до активів підприємства, наприклад, до серверів і мережевого обладнання, доступ лише ключовому персоналу.
- Керування ключами доступу до точок входу – двері, вікна, хвіртки.
- Інтеграція із системами відеоспостереження.

1.3.2 Системи відеоспостереження

Однією із головних частин системи безпеки є відеоспостереження. Камери є частиною будь-якої хорошої стратегії безпеки, комерційні системи відеоспостереження дають можливість бачити картину того, що відбувається у будівлі. Перелічимо основні характеристики систем відеоспостереження, що використовуються на підприємствах [7]:

- Налаштування нічного бачення або слабкого освітлення – системи відеоспостереження можуть бути оснащені нічним баченням, це особливо корисно для моніторингу в неробочий час або на відкритому просторі. За допомогою цього можливо отримувати чіткі зображення навіть у темряві.
- Можливість дистанційного панорамування/нахилу/масштабування – інколи може знадобитися можливість збільшувати, нахиляти або змінювати огляд камери. Ці типи камер зазвичай дорожчі, ніж простіші купольні камери.
- Стійкі до погодних умов – якщо система камер встановлена камер на вулиці, знадобиться апаратне забезпечення, яке може витримувати погодні умови.
- Вбудований датчик руху – така система відеоспостереження, записуватиме відео, лише якщо виявить рух у кадрі. Це може допомогти зменшити витрати на зберігання даних і вимоги до мережі підприємства.
- Інтеграція з мережею підприємства – камера може записувати записи у хмарне сховище чи сервер розташований у будівлі підприємства. Такий

підхід спрощує підключення систем контролю доступу, сигналізації, платформ безпеки та інших програмних засобів для більш цілісного підходу до безпеки.

Існує велика маса камер для систем відеоспостереження, але є дві основні системи камер які використовуються на підприємствах: дротова та бездротова. Перелічимо їх основні відмінності [7]:

- Дротові комерційні камери безпеки потребують кабель, який проходить до центрального концентратора, що забезпечує передачу даних та відео. Основна перевага дротової системи відеоспостереження для бізнесу полягає в тому, що немає необхідності хвилюватися про слабкий чи поганий сигнал. Оскільки з'єднання здійснюється за допомогою коаксіальних кабелів або кабелів PoE, запис відеоспостереження завжди буде надійним, доки є живлення .
- Бездротові камери надсилають відео через Ethernet або Wi-Fi. Бездротові камери можна підключати безпосередньо до джерела живлення або працювати від акумуляторів. Бездротові системи відеоспостереження для бізнесу часто більш дешеві у встановлені встановлення, ніж дротові.

За принципом передачі відеосигналу системи камер бувають:

- Аналогові відеокамери – ці типи систем відеоспостереження використовують коаксіальні кабелі для передачі відео та даних. Налаштування системи комерційних камер відеоспостереження є досить простим, оскільки кожна камера під'єднана до джерела живлення та направлена на локальний відеореєстратор (DVR). Аналогові системи відеоспостереження є хорошим способом надати можливість візуального моніторингу. Хоча аналогові камери відеоспостереження часто дешевші за одиницю, проте вони можуть бути дорожче за рахунок вартості кабелів та мають обмежену функціональність аналітики та запису порівняно із цифровими відеокамерами.
- IP-відеокамери (цифрові камери) – це камери мережевого відеоспостереження передають зображення через Ethernet, і багато з них не

потребують додаткового джерела живлення чи кабелю (PoE). Це робить системи IP-камер легшими для встановлення, ніж аналогові або бізнес-системи відеоспостереження. Крім того, вони підтримують більш високоякісне відео, деякі постачальники IP-камер підтримують якість відео до 4k із більшими можливостями масштабування. Однак системи IP-камер часто дорожчі за аналогові системи відеоспостереження. Завдяки вбудованому шифруванню та стисненню даних, а також заходам мережевої безпеки IP-системи відеоспостереження для бізнесу пропонують більшу надійність і безпеку порівняно з традиційними системами.

Комутатори Power-over-Ethernet (PoE) забезпечують як живлення, так і передачу даних через один мережевий кабель для систем IP-камер. Однією з переваг використання комутатора PoE для комерційного відеоспостереження є те, що його легше встановлювати, обслуговувати та усувати несправності. Керовані комутатори PoE забезпечують більш широкі налаштування, що корисно для керування вихідною потужністю для кожної камери. Оскільки комутатори PoE мають IP-адресу, можливо дистанційно заходити в систему через веб-браузер, щоб перевірити стан системи, налаштувати параметри та оптимізувати роботу систем відеоспостереження.

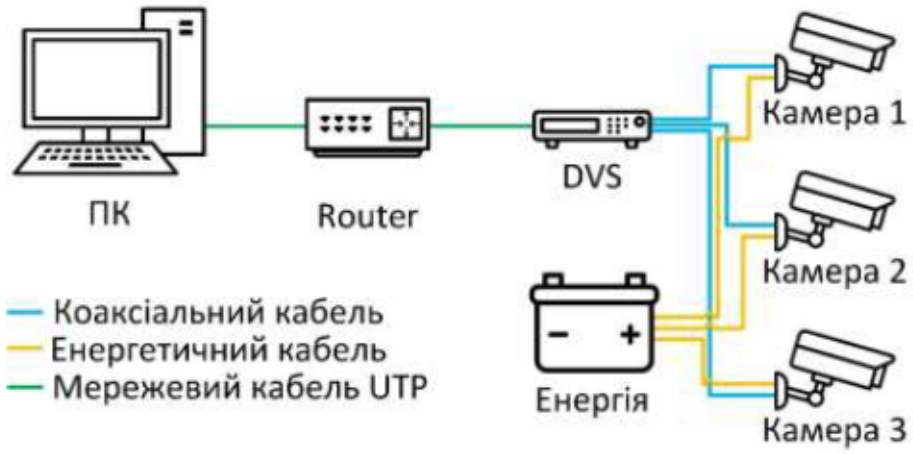


Рисунок 1.2 Схема підключення аналогової камери

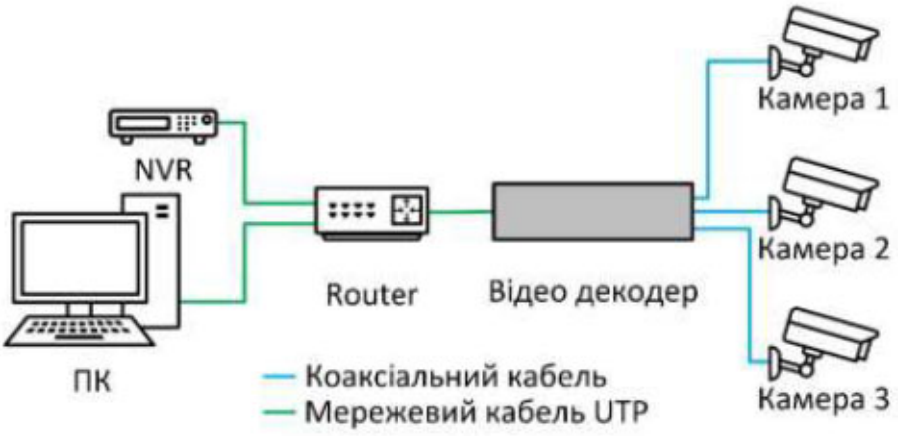


Рисунок 1.3 Схема підключення цифрової IP-камери

1.3.3 Інформаційна безпека підприємства

Система інформаційної безпеки підприємства (кібербезпека) – це практика захисту даних і ресурсів компанії від кіберзагроз. Кібербезпека повинна забезпечувати локальний захист даних та передачу даних між мережами, пристроями та кінцевими користувачами. Кібербезпека підприємства не тільки має справу з поширеними проблемами безпеки, такими як атаки відмови в обслуговуванні (DoS), соціальна інженерія та вразливість програмного забезпечення. Але окрім цього також потрібно враховувати, як дані передаються між пристроями та мережами всередині організації в цілому, для забезпечення комплексної системи безпеки [8, 9].

Для успішного створення системи інформаційної безпеки на підприємстві необхідно дотримуватись трьох основних принципів [8]:

- Доступність даних. Доступність забезпечує ефективний та надійний доступ до інформації авторизованим особам. Мережеве середовище повинно бути передбачуваним із метою отримати доступ до інформації та даних, коли це необхідно. Якщо буде збій система повинна мати можливість відновлення і таке відновлення також має бути забезпечене таким чином, щоб це не впливало на інші дані негативно.
- Конфіденційність інформації. Тобто введення в дію контролю доступу, щоб гарантувати надійний рівень безпеки для даних підприємства, активів та

інформації на різних етапах бізнес операцій для запобігання небажаного або несанкціонованого доступу. Конфіденційність повинна забезпечуватися при збереженні інформації, а також пересиланні через інші організації незалежно від її формату.

- Цілісність даних. Інформація підприємства повинна бути внутрішньо та зовні послідовною. Цілісність також гарантує запобігання спотворенню інформації.

Опишемо види сучасних інформаційних загроз, що можуть бути на підприємстві [9]:

- SQL-ін'єкція – ця атака спрямована безпосередньо на сайт і базу даних підприємства. У разі успіху зловмисник може ввести фрагмент коду SQL, який під час виконання надає доступ до конфіденційної інформації або навіть надає права редагування бази даних.
- DDoS-атака (розподілена відмова в обслуговуванні) – це пряма атака на мережу підприємства. Ціль атаки сервер, що б перевести його в не робочий режим для різних цілей. Зловмисники також можуть використовувати цей тип атаки, щоб приховати інші вектори атак, які складніше ідентифікувати.
- Витік даних – це є порушенням безпеки. Конфіденційні дані викрадаються або копіюються особами, які не мають на це повноважень. Ненадійні паролі часто можуть бути першопричиною цього, але це також може бути спричинено: розсилкою шахрайських листів (фішинг), зловмисне забезпечення на переносних носіях інформації або за допомогою соціальної інженерії.

Інформаційним загрозам і витокам даних можна запобігти та пом'якшити їх за допомогою належних практик корпоративної інформаційної безпеки, таких як розробка та визначення сфери безпеки, вивчення корпоративної архітектури та використання традиційних методів кібербезпеки. Опишемо методи що можуть захистити підприємство від інформаційних загроз [9]:

- Багатофакторну автентифікацію для співробітників підприємства – це потужна функція для запобігання доступу неавторизованих користувачів до конфіденційних даних. Для найбільш безпечного входу користувачів слід використовувати такі елементи, як біометрія, SMS/текстові повідомлення, електронні листи.
- Постійне навчання співробітників, щоб зменшити людські помилки під час завантажень або загроз соціальної інженерії. Одним із найважливіших аспектів безпеки підприємства є навчання співробітників тому, як залишатися в безпеці в Інтернеті. Захист корпоративної мережі виходить за рамки команди інформаційних технологій — кожен має знати про політику безпеки, правила відповідності та потенційні вразливості, такі як фішинг або схеми соціальної інженерії.
- Політика надійних паролів – це використання таких практик: довгі паролі (від 15 символів), комбінація різних символів, без використання словникових слів, регулярна заміна паролів (раз на місяць), використання менеджер паролів.
- Деталізована перевірка всіх потенційних загроз, включаючи персональні пристрої співробітників, використання тимчасових паролів, двофакторна або багатофакторна автентифікація.
- Створення резервних копій даних – є одним із найкращих засобів захисту особистих і ділових даних від атак програм-вимагачів. Забезпечити захист даних підприємства можна, запровадивши постійне резервне копіювання. Можливе використання хмарного сховища або копія своїх даних на сервері підприємства. Якщо систему було зламано, то можливо відновлення даних.

Окремо слід розглянути таку важливу ланку у забезпечені інформаційної безпеки підприємства як мережевий екран (Firewall). Мережевий екран чи брандмауер — це мікропрограма або програмне забезпечення, яке керує та контролює правила щодо того, які типи пакетів даних можуть проходити в мережу підприємства, а також інші аспекти безпеки мережі. Мережевий брандмауер є

найважливішим будівельним блоком інфраструктури кібербезпеки будь-якого підприємства.

Є два основні варіанти захисту мережі за допомогою мережевих екранів. Ці два варіанти мають свої плюси та мінуси.

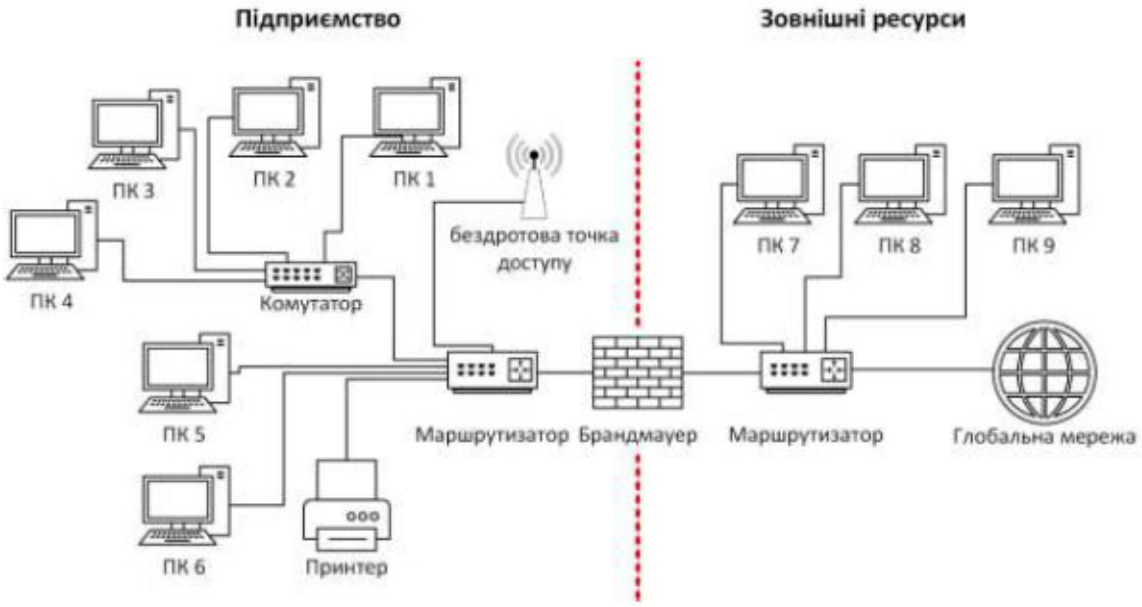


Рисунок 1.4 – Приклад використання мережевого екрану на підприємстві

Мережевий брандмауер є основним типом брандмауера. Мережевий брандмауер розташовується безпосередньо між двома або більше мережами. Зазвичай це лінія розмежування між локальною мережею (LAN) і глобальною мережею (WAN) , але контури мережевого брандмауера можуть бути визначені так, як підприємство вважає за потрібне. Мережевий екран, як правило, може бути частиною спеціального або універсального обладнання для моніторингу мережевого трафіку, але існують також повністю віртуальні мережеві рішення.

Брандмауери можуть запобігти наступним загрозам безпеки підприємства [9]:

- Віддалений вхід неавторизованих користувачів.
- Програмами, які встановлюють функції, що дозволяють прихований доступ.

- Відмова в обслуговуванні (DDoS), коли мережа підприємства переповнена згенерованим мережевим трафіком, що спричиняє сповільнення або збій комп'ютерів у мережі.
- Віруси та хробаки, що поширюються мережею, невеликі програми, які можуть поширюватися мережею на інші незахищені комп'ютери.

Мережеві екрани веб-програм (WAF) — це тип програм, які працюють безпосередньо з веб-програмами. Брандмауер веб-додатків розташований перед веб-додатками та відстежує як вхідний, так і вихідний веб-трафік. Брандмауери веб-додатків, оскільки вони ретельніше аналізують дані, ніж мережеві брандмауери. Опишемо їх особливості:

- Проста конфігурація – налаштування та специфіка функціональність веб додатків сумісні із брандмауерами веб-додатків, і їх можна оновлювати на ходу, щоб відповідати вимогам нових цифрових загроз або обладнання, що було додане до корпоративної мережі.
- Сумісність – брандмауер на основі веб-додатків створений для будь-якої веб-програми. Це означає, що бізнес, який ведеться онлайн через браузер, може бути захищений незалежно від програми. Складні операції, які не можуть дозволити собі ізолювати свої мережі, будуть задоволені гнучкістю, яку забезпечують брандмауери веб-додатків.

1.3.4 Пожежна безпека

Система пожежної сигналізації на підприємстві призначена для сповіщення про надзвичайну ситуацію, щоб люди могли вжити заходів для захисту себе, персоналу та підприємства в цілому.

В основі системи пожежної безпеки є пристрої виявлення, від складних інтелектуальних детекторів диму до простих блоків із ручним керуванням. Існує широкий спектр різних типів, опишемо їх [3]:

- Теплові сповіщувачі – може працювати на основі визначення фіксованої температури, де він запускає тривогу, якщо температура перевищує попередньо встановлене значення, або вони можуть працювати на швидкості зміни температури.
- Датчики диму – існує три основних типи детекторів диму, за видом виявлення диму: іонізація, розсіювання світла, затемнення світла.
- Детектори чадного газу – детектори чадного газу також відомі як пожежні сповіщувачі CO, це електронні сповіщувачі, які використовуються для вказівки на спалах пожежі шляхом визначення рівня чадного газу в повітрі.
- Мультисенсорні детектори – такі сповіщувачі поєднують вхідні дані від оптичних і теплових датчиків і обробляють їх за допомогою складного алгоритму, вбудованого в схему сповіщувача. При опитуванні панелі керування сповіщувач повертає значення на основі комбінованих відгуків оптичного та теплового датчиків. Вони розроблені таким чином, щоб бути чутливими до широкого діапазону пожеж.
- Ручні сповіщувачі – ручний сповіщувач або сповіщувач розбитого скла — це пристрій, який дозволяє персоналу підняти тривогу, зламавши крихкий елемент на панелі; це викликає тривогу.

Розглянемо детально датчики диму:

- Іонізаційний димовий сповіщувач зазвичай містить дві камери. Перший використовується як еталон для компенсації змін температури навколишнього середовища, вологості або тиску. Друга камера містить радіоактивне джерело, зазвичай альфа-частинку, яка іонізує повітря, що проходить через камеру, де струм протікає між двома електродами. Коли дим потрапляє в камеру, потік струму зменшується. Це падіння потоку струму використовується для ініціювання тривоги.
- Світлорозсіювальний димовий сповіщувач – працює за ефектом Тиндаля ; фотоелемент і джерело світла відокремлені один від одного затемненою камерою, щоб джерело світла не потрапляло на фотоелемент. Проходження

диму в камеру призводить до того, що світло від джерела розсіюється і потрапляє на фотоелемент. Вихід фотоелемента використовується для ініціювання тривоги.

- У детекторі диму, що затемнює світло, дим перешкоджає променю світла між джерелом світла та фотоелементом. Фотоелемент вимірює кількість світла, яке він отримує. Зміна потужності фотоелемента використовується для ініціювання тривоги.

Системи пожежної сигналізації можна розділити на чотири основні типи, перелічимо їх [3].

- Традиційні системи пожежної сигналізації – у такій системі пожежної сигналізації фізичні кабелі використовуються для з'єднання кількох сповіщувачів і сповіщувачів, сигнали від яких направляються назад на головний блок керування.
- Адресні системи пожежної сигналізації – принцип виявлення адресної системи такий самий, як і звичайної системи, за винятком того, що кожному сповіщувача присвоюється встановлена адреса, і панель керування може потім точно визначити, який сповіщувач або сповіщувач ініціював тривогу.
- Інтелектуальні системи пожежної сигналізації – у такій системі кожен сповіщувач фактично містить власний мікроконтролер, який оцінює навколишнє середовище та повідомляє панелі керування. По суті, інтелектуальні системи набагато складніші та включають набагато більше засобів, ніж звичайні або адресні системи. Їхнє основне призначення — допомогти запобігти виникненню помилкових тривога.
- Бездротові системи пожежної сигналізації – останнім типом системи, яку ми розглянемо, є бездротова система пожежної сигналізації. Це ефективна альтернатива традиційним дротовим системам пожежної сигналізації для всіх застосувань.

Технічні функції системи пожежної сигналізації [3]

- виявити пожежу на ранніх стадіях її розвитку;
- передавати сигнали тривоги на пристрої оповіщення про пожежу;
- формувати сигнали керування системами протипожежного захисту та іншим інженерним обладнанням, задіяним у пожежно-рятувальних роботах;
- сигналізувати про виявлену несправність, яка може негативно вплинути на нормальну роботу системи.

Рисунок 1.5 – Приклад підключення пожежної сигналізації на підприємстві

ВИСНОВОК

У ході першого розділу було оглянуто актуальність систем безпеки сучасних підприємств. Розглянуто типові загрози для них, внутрішні та зовнішні атаки на фізичну та інформаційну безпеку підприємства. Також було проведено огляд популярних протоколів передачі даних у системах безпеки, їхні дротові та бездротові версії, дальність та енергоефективність.

В подальшому були проаналізовані сучасні методи та принципи комлексного захисту підприємства із організацією систем безпеки у декількох сферах: фізичній, інформаційній та пожежній безпеці. Окремо також було розглянуто відеоспостереження, оцінено його важливість для комплексного захисту, розглянуто два типи камер – аналогові та IP. Для кожного типу камер приведені схеми підключення та їх особливості. У ході розгляну побудови інформаційного захисту також було приділено увагу мережевим брандмауерам, його типам та варіантів захисту корпоративної мережі.

2 РОЗРОБЛЕННЯ ПРОЕКТУ СИСТЕМИ БЕЗПЕКИ

2.1 Загальна структура та стан мережі підприємства

2.1.1 Опис структури підприємства

Підприємство ТОВ «Індустріальні Системи Автоматизації» займається ремонтом, налаштуванням та подальшим обслуговуванням комп'ютерної техніки. Роботи виконуються як в середині офісної будівлі так і на виїзді у клієнта. Окрім цього підприємство також займається продаванням комп'ютерного устаткування та програмного забезпечення [10].

Доцільно розглянути карту підприємства на якому проводитися модернізації системи безпеки (рис. 2.1).

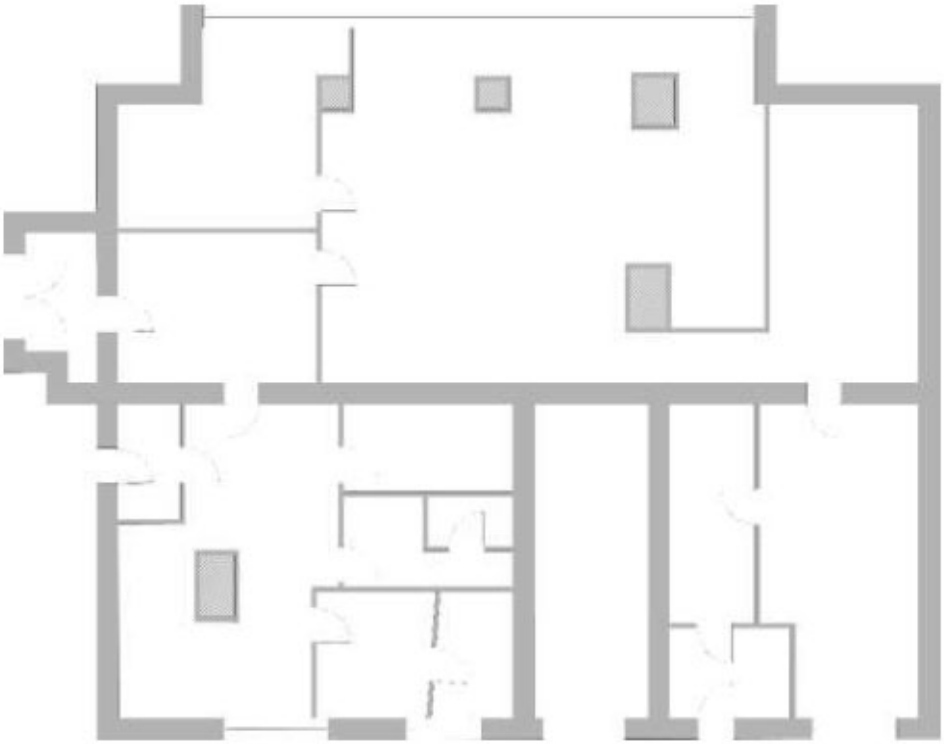


Рисунок 2.1 – Карта підприємства

2.1.3 Мережа підприємства

Наявну мережу підприємства являє собою топологію «зірка» усі вузли підключаються до мережевого маршутизатору, він у свою чергу надає доступ у глобальну. Комп'ютерну мережу можна поділити на два сегменти:

- 100 Мбіт/с, для підключення більшості обладнання та звичайних користувачів.
- 1 Гбіт/с, для підключення серверів та специфічного обладанння, що потребує високої швидкості.

У складі мережі підприємства є два обладнання, що здатні до створення точки бездротового доступу це маршрутизатори RB951G-2HnD та WF2780. RB951G-2HnD має 2.4 ГГц діапазон. WF2780 працює у двох діапазонах у 2.4 ГГц та 5 ГГц. Це надає можливості підключати як застаріле обладнання так і сучасне.

Все мережеве обладнання підключене за допомгою комунікаційного обладнання, а саме через комутатори DES-1024D та DGS-1008D та маршрутизатори RB951G-2HnD.

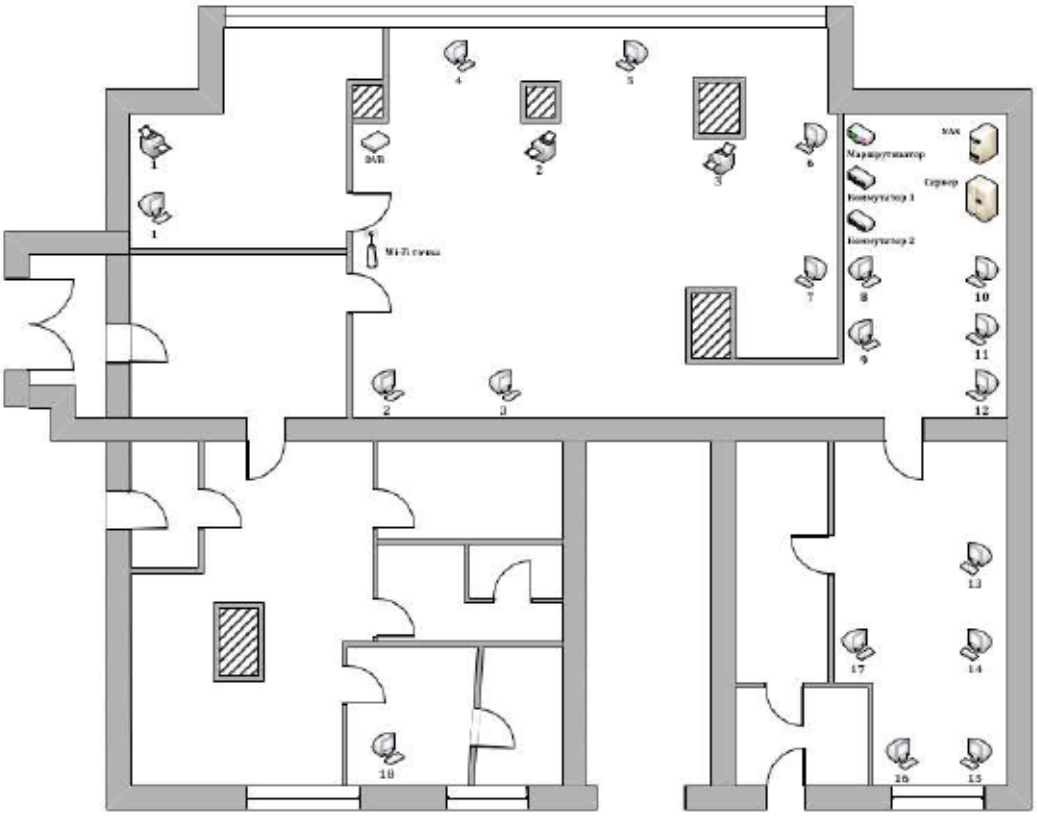


Рисунок 2.2 – Обладнання, що наявне на підприємстві

Проведемо детальний опис мережевого обладнання, що присутнє на підприємстві (табл. 2.1).

Таблиця 2.1 – Необхідні швидкості для обладнання мережі

Тип обладнання	Назва моделі
Сервер	Dell PowerEdge R815
3 мережеві принтери	OKI MB770; OKI B432DN; KYOCERA ECOSYS FS-1025MFP
Маршрутизатор для Wi-Fi доступу	Mikrotik RB951G-2HnD
2 мережевих комутатори	D-Link DES-1024D
Мережеве сховище	D-Link DGS-1008D
18 ПК	-

Загалом мережа підприємства має 18 персональних комп'ютерів, 3 мережевих принтери, сервер, маршрутизатор та одне мережеве сховище (NAS).

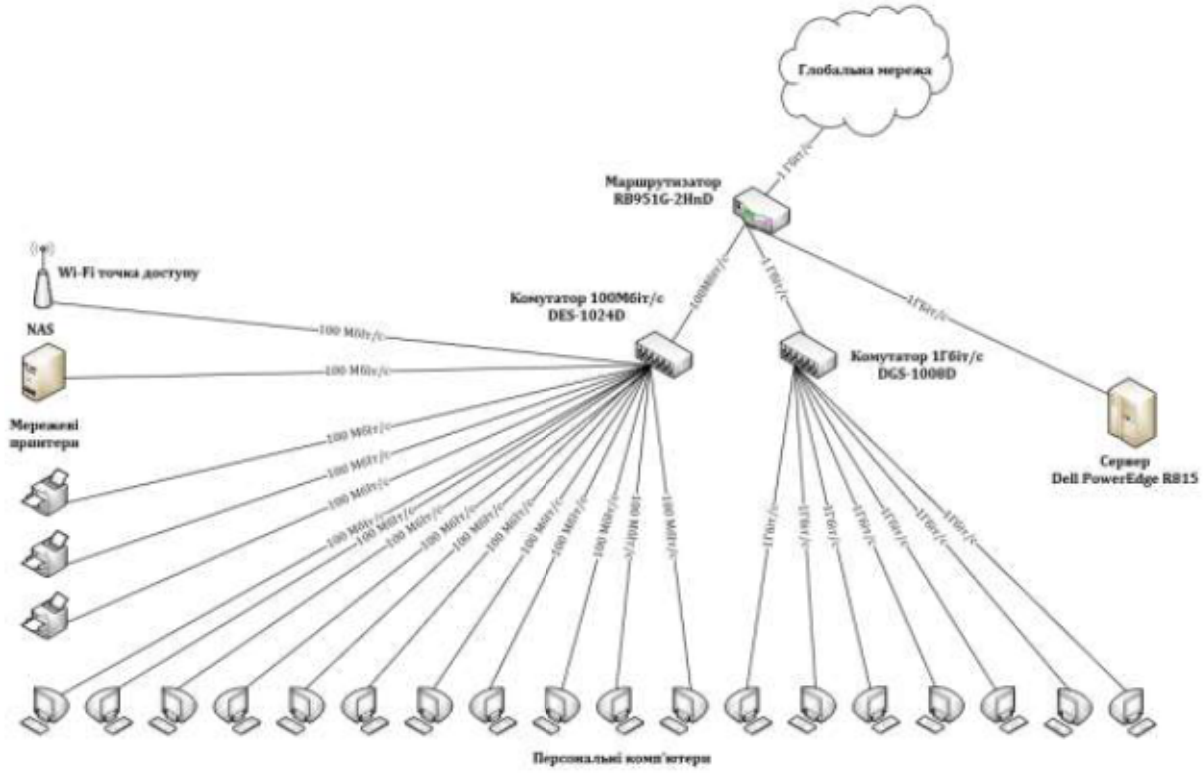


Рисунок 2.3 – Загальна топологія мережі підприємства

2.2 Опис проекту системи безпеки

2.2.1 Вимоги до охоронної системи

Система охоронної сигналізації на підприємстві повинна забезпечувати такий функціонал для фізичного захисту підприємства[1,2,5]:

- постановку під охорону та зняття з охорони приміщень або груп приміщень (залежно від їхньої категорії та функціонального призначення) як централізовано з робочого місця оператора систем безпеки у приміщенні охорони біля головного входу, так і децентралізовано за допомогою периферійних пультів;
- виявлення та фіксування фактів відчинення дверей, розбиття скла, пересування порушників у приміщеннях об'єкта, зданих під охорону;
- візуальне відображення стану сповіщувачів, охоронних зон та шлейфів сигналізації на АРМ оператора систем безпеки;
- дублювання тривожних повідомлень у систему безпеки;
- Формування сигналів для системи управління доступом;
- формування сигналів для охоронного відеоспостереження.
- Формування сигналів для охоронного освітлення;
- фіксування інформації про всі прийняті сигнали тривоги в базі даних із зазначенням дати, часу та адреси та ведення протоколу роботи.

Система керування доступом повинна забезпечувати:

- ідентифікацію персоналу та ранжоване автоматичне управління доступом до зон та приміщень об'єкта;
- ручне керування (розблокування) дверей, обладнаних пристроями керування доступом з пульта керування на посту охорони;
- формування сигналів для підсистеми охоронної сигналізації у разі виникнення нештатних ситуацій (спробах злому) у системі управління доступом;

Проектування системи відеонагляду повинно включати в себе [9]:

- визначення архітектури системи відеоспостереження;
- підбір обладнання з урахуванням можливого розвитку системи;
- розрахунок кутів огляду камер;
- підбір об'єктивів відеокамер;
- розрахунок місткості бази даних;
- об’єкти контролю доступу (двері, вікна, обладнання).

2.2.2 Вимоги до інформаційної охорони

Перелічимо основні вимоги до інформаційної безпеки на підприємстві [10, 11] :

- Захист серверів та конференційних даних на них
- Авторизація співробітників на персональних комп’ютерах.
- Антивірусне забезпечення
- Розмежування доступу до файлів.
- Мережевий екран

2.2.3 Вимоги до пожежної безпеки

Система пожежної сигналізації має забезпечувати [3]:

- Виявлення та фіксування фактів появи вогнищ загоряння, задимленості, підвищення температури;
- Формування сигналів для системи безпеки об'єкта;
- Формування сигналів для системи управління доступом;
- Формування сигналів для охоронного телебачення з пріоритетного включення телевізійних зображень тривожної зони та прилеглих зон;
- Формування сигналів для пристроїв автоматичного пожежогасіння, систем кондиціювання, вентиляції, димовидалення та ін;
- Фіксування інформації про всі прийняті сигнали тривоги в базі даних.

2.3 Аналіз та вибір засобів та обладнання для системи безпеки

2.3.1 Контролери охоронної мережі

Головний контролер системи безпеки або охоронної мережі – це такий прилад, котрий забезпечує управління іншими пристроями, він є центральним елементом системи безпеки та контролю доступу на підприємстві. За допомогою контролеру можлива робота інших сповіщувачів (датчиків), окрім цього він запускає на виконання спеціальні сценарії у разі виявлення різних подій. Зазвичай контролер має з'єднання із глобальною мережею Internet та локальною мережею об'єкту, що охороняється. Усе інше обладнання підключаєтеся до контролеру за допомогою проводових чи без проводових інтерфейсів.

Для вибору контролеру, нижче приведемо декілька можливих моделей контролерів для системи безпеки підприємства.

Контролер Ajax Hub – головний пристрій у системи безпеки екосистеми фірми Ajax. Забезпечує та контролює працездатність всіх сповіщувачів Ajax і в разі чого моментально відправляє сигнал про подію на пульт охорони. Обробляє дані що присилають датчики в зашифрованому вигляді, проводить аналіз цих даних і в разі тривоги запускає виконання різноманітних сценаріїв – наприклад при тривозі. У ролі бездротового інтерфейсу використовує протокол Jeweller для моніторингу роботи датчиків та оперативного реагування на тривогу. Може перекидавати систему зв'язку на інші частоти при виявленні глушіння[13].

Приведемо характеристики контролеру Ajax Hub у таблиці 2.1.

Таблиця 2.1 – Характеристики Ajax Hub

Характеристика	Значення
Бездротовий протокол	Z-Wave
Максимальна дальність зв'язку	2000
Максимальна кількість пристроїв	100
Робоча частота	868,0 - 868,6 МГц
Додаткові можливості	Опитування датчиків 12-300с, підтримка до 50 кімнат та 9 груп

Контролер Ajax Hub 2 Plus – більш покращена версія попереднього контролеру. Використовує 4 канальний зв'язок та підтримує швидкісні протокол мобільної мереж 4G LTE. За допомогою цього можливо підключення пристрою до окремих інтернет-провайдерів через інтерфейси Ethernet і Wi-Fi. Якщо цього не достатньо є можливість підключення до двох мобільних операторів. За рахунок покращеної роботи цьому автоматичне перемикання між каналами радіозв'язку займає декілька секунд [13].

Приведемо характеристики контролеру Ajax Hub 2 Plus у таблиці 2.3.

Таблиця 2.3 – Характеристики Ajax Hub 2 Plus

Характеристика	**Значення**
Бездротовий протокол	Wi-Fi 2.4 ГГц (802.11 b / g / n), Z-Wave
Максимальна дальність зв'язку	2000
Максимальна кількість пристроїв	200
Робоча частота	868,0 - 868,6 МГц
Додаткові можливості	Опитування датчиків 12-300с, підтримка до 100 камер та 25 груп приміщень GSM-модуль для двох SIM-карт з підтримкою 2G і 3G, LTE

Контролер GSM OKO-7S – забезпечує дистанційне управління, контроль і оповіщення стану віддаленого об'єкта за допомогою мобільної мережі. Має не великий функціонал, але це компенсується його низькою вартістю. Загалом призначений для контролю невеликий територій чи як бюджетне рішення. Може керувати сиреною тривоги. Налаштування може бути за допомогою мобільного застосунку [14].

Приведемо характеристики контролеру ОКО-7S у таблиці 2.4.

Таблиця 2.4 – Характеристики ОКО-7S

Характеристика	Значення
Бездротовий протокол	GSM
Максимальна кількість входів	5
Макс. кількість вихідних каналів	3
Додаткові можливості	Робота виходів за розкладом, користувачів – 8, груп для датчиків - 8

Контролер ОРІОН NOVA L — нова серія GSM контролерів із розширеним функціоналом керування типу «розумний будинок». За допомогою нього можливо організувати автономну, надійну систему безпеки із віддаленим керуванням. Можливість підтримувати до 16 зон, за потреби може бути збільшена до 64 зон. Модель може працювати одночасно із 8 клавіатурами введення, а також є додатковий вихід під сирени сповіщення. Загалом є по два релейних та транзисторних виходи. Налаштування контролеру відбувається за допомогою програми на телефоні чи комп'ютері, також підтримується налаштування через клавіатуру введення.

Приведемо характеристики контролеру Оріон NOVA L у таблиці 2.4.

Таблиця 2.4 – Характеристики Оріон NOVA L

Характеристика	Значення
Бездротовий протокол	Ethernet/Wi-Fi, GSM
Максимальна кількість зон	16 із розширення до 64
Додаткові можливості	Пам'ять до 1000 подій, можливість розширення до 64 зон, 64 номери оповіщення

Рисунок 2.4 – Обраний контролер для охоронної мережі Ajax Hub 2 Plus

У ході аналізу вищезгаданих контролерів було обрано контролер Ajax Hub 2 Plus, оскільки він має гарну екосистему фірми Ajax Systems, та, що головніше – кращі характеристики за свою ціну, ніж конкуренти: підтримувані протоколи передачі даних, кількість датчиків, зон контролю, можливих сценаріїв. У подальшому обладнання із таким контролером можливо буде легко модернізувати без внесення суттєвих змін у структуру охоронної мережі підприємства.

2.3.2 Датчики руху, присутності людини

Датчик руху – це такий прилад, що може виявляти переміщення різних об'єктів, тому його використовують для контролю доступу та автоматичного запуску дій сценаріїв, відповідно до переміщення об'єктів у середовищі.

Перелічимо асортимент доступних датчиків із вказанням їх особливостей у таблиці 2.5 [13, 15].

Таблиця 2.5 – Асортимент можливих датчиків руху

Датчик	Характеристика	Значення
ATIS-804DW	Тип виявлення	Інфрачервоний
	Тип радіоканалу	433 МГц
	Область сканування	8 м / 110°
Ajax MotionCam	Тип виявлення	Інфрачервоний
	Тип радіоканалу	Z-Wave
	Область сканування	12 м / 88.8°
Aqara Human Body Sensor	Тип виявлення	Інфрачервоний
	Тип радіоканалу	ZigBee

Продовження таблиці 2.5 – Асортимент можливих датчиків руху

	Область сканування	170°
Ajax MotionProtect	Тип виявлення	Інфрачервоний
	Тип радіоканалу	Z-Wave
	Область сканування	9 м / 88.8°
FIBARO Motion Sensor	Тип виявлення	Інфрачервоний
	Тип радіоканалу	Z-Wave

Рисунок 2.5 – Обраний датчик руху Ajax MotionProtect

Виходячи із вимог, що висуваються до системи безпеки, доцільно обрати тип датчиків руху – Ajax MotionProtect, оскільки він має гарні характеристики за свою ціну та просте встановлення і можливість подальшого налаштування через контролер. Також можливо розглянути інший Ajax MotionCAM які надають фотофіксацію, проте враховуючи подальше встановлення камер на підприємстві, вони будуть надлишкові.

2.3.3 Датчики відкриття дверей та RFID сенсори

Датчик відкриття дверей (вікна) є пристроєм, завданням якого є контроль проникнення в приміщення. Найпоширенішою та дуже ефективною, з ймовірністю виявлення проникнення понад 99%, модифікацією є магнітоконтактний сповішувач або магнітний датчик відкриття дверей чи вікна.

Опишемо деякий асортимент датчиків відкриття дверей та вікон:

- Ajax DoorProtect – сповішувач призначений для моніторингу стану дверей та вікон. Цей датчик є бездротовим та обладнаний роз'ємом для підключення

інших додаткових датчиків по проводу, тобто він може бути в ролі бездротового ретранслятору для проводових датчиків. Чутливість сповіщувача близько 2 см. Автономність забезпечується на рівні до 7-ми років від батарейки типу CR123A.

- Ajax DoorProtect Plus - датчик виявлення відкриття вінок дверей. Загалом покращена версія попереднього датчика. Аналогічний базовій моделі, але має ще здатність виявляти удари та зсув свого місцеположення.
- Aqara Window and Door Sensor – датчик, що має можливість інтеграції із системами «smart house», наприклад: MiHome, Apple Home, Aqara Home. Особливістю є робота по популярному протоколу телеметрії – ZigBee.
- ATIS-19DW – бездротовий датчик відчинення дверей [15]. Максимальна дальність виявлення 1 см. Робоча частота: 433 МГц, дальність передачі до 100 м. Може працювати спільно із GSM сигналізацією фірми ATIS.
- FIBARO Door/Window Sensor 2 – це бездротовий датчик відкриття дверей, має сумісність із протоколом Z-Wave Plus. Також у сповіщувачі є вбудований датчик температури.

Для захисту підприємства було обрано базову модель Ajax DoorProtect вона має усі необхідні характеристики для своєї ролі у системі безпеки та можливість інтеграції із обраним для проекту головним контролером охорони.

RFID мітка або смарт-картка – пластикова безконтактна карта, елемент радіочастотної ідентифікації об'єктів. У конструкції RFID картки є мікросхема, яка відповідає за зберігання інформації та антена, що передає сигнал зчитувачу. У такому прихованому чіпі зберігається унікальний ідентифікатор, яким у базі даних можна прочитати чи записати потрібну інформацію [8].

Опишемо деякий асортимент RFID смарт карток для контролю доступу:

- Ajax Pass Black – RFID картка за допомогою якою користувач може провести свою безконтактну ідентифікацію, встановити сигналізацію на охорону або зняти з неї. За допомогою цієї картки можливо керувати станом охорони об'єкту можна без наявного облікового запису у системі Ajax або знати секретний пароль безпеки. Для розблокування достатньо лише

піднести смарт-картку до зчитувача KeyPad Plus, і система буде знята або встановлена у режим охорони. Підтримувані стандарти роботи: ISO 14443-A на частоті 13,56 МГц.

- Tecsar Trek Mifare – багатофункціональна смарт-карта. Має 8 КБ для корисних даних чи даних налаштувань. Межа гарантованого спрацьовування – не більше 10 см до зчитувачів. Дані поділяються на 16 секторів, кожен із них захищений різними ключами типу А та Б, ці сектори можуть бути запрограмовані на різні функції такі як: запис чи зміна блоку даних. Підтримує стандарт ISO 14443.
- Atis MiFare card – картка для безконтактної ідентифікації її робоча частота популярний діапазон 13.56 МГц що дозволяє працювати із більшістю зчитувачів стандарту ISO 14443.

2.3.4 Датчики розбиття скла

Звуковий датчик розбиття скла - це такий сповіщувач, що виявляє звук розбити вікна, біля якого він встановлений. Головне що повинен зробити датчик це – моментально відреагувати на звук розбиття скла та запустити відповідні сценарії реагування. Над даний момент є два типи сповіщувачів. Перший тип чутливий до звуку розбиття, другий – на звук удару, тобто вібрацію. Є ще гібридні датчики котрі реагують відразу як на звук так і на удар. Датчики мають спеціальну мікросхему для швидкого реагування на звук.

Опишемо деякий асортимент датчиків розбиття скла:

- GlassProtect – сповіщувач, що не потребує проводів може розпізнати на відстані до 9 метрів звук розбитого скла [11]. Уразі спроби проникнення правопорушника в приміщення шляхом розбиття скла, система відразу відреагує надіславши повідомлення на головний контролер охорони. Також наявний захист від помилкових спрацювань – машини та звук домашніх тварин не буде створювати проблеми.

- SATEL MGD-300 – цифровий датчик розбиття скла призначений для виявлення розбиття листового, загартованого або ламінованого скла. Плавне регулювання чутливості дозволяє точно налаштувати його чутливість. MGD-300 використовує багаточастотний аналіз спектру акустичного сигналу, що робить його стійким до випадкових шумів, які можуть виникати під час нормальної роботи на вулиці чи в приміщенні.
- Satel INDIGO – сенсор виявлення розбиття скла оснащений бездротовим інтерфейсом. Із особливостей: може визначити момент падіння напруги живлення нижче 9 В та відправити повідомлення на головний пульт охорони. Можливо налаштовувати межі спрацьовування датчику, який працює за принципом виявлення двох сигналів – високочастотного та низькочастотної компоненти звукового спектру, це дозволяє зменшити спрацювання від помилок. Цей сенсор може працювати із різними типами скла, багатошаровими, звичайним чи загартованим.
- Trinix TRX-1220BG – це пасивний датчик оснащений мікрофоном для виявлення розбиття скла. Призначений для установки всередині приміщень. Завдяки функції шумозаглушення та виявленню помилкових спрацьовувань, модель датчику можна встановлювати в приміщеннях з високим рівнем фонового шуму. Дистанція виявлення у приміщенні розбиття скла сягає до 10 метрів.
- Датчик разбиття Crow GBD-2 – Високоякісний твердотільний бездротовий детектор. Працює у діапазоні частот 868/916,5 МГц. Сенсор виявлення зроблений так, щоб його можна було встановлювати безпосередньо на стіні біля скла, а його принцип дії дозволяє захищати дистанційно відразу кілька вікон. Є два налаштування чутливості для низької та високої частоти. Дальність виявлення до 12 м.

Рисунок 2.6 – Обраний датчик розбиття скла GlassProtect

У ході аналітичного вибору було обрано датчик розбиття склад GlassProtect оскільки він має гарну дистанцію виявлення звуку розбиття скла та систему шумозаглушення, що б мати захист від помилкового спрацювання.

2.3.5 Системи відео спостереження

Система відеоспостереження дозволяє проводити цілодобовий моніторинг приміщення від різного типу загроз із подальшою відеофіксацією. Така система складається із відеокамер цифрового чи аналогового типу та відповідного їм пристрою – відеореєстратору, його призначення обробляти вхідні потоки даних та зберігати отриманий трафік відео.

Приведемо список асортименту відеокамер для спостереження [9, 17]:

- IP камера Tapo C310 –цифрова камера яка має 3МП розподільчої здатності. Може бути підключена двома способами проводовим за допомогою Ehternet кабелю та бездротовим за допомогою Wi-Fi. Присутня додаткова можливість нічної підсвітки що забезпечує до 30 метрів видимості. Камера може відправляти повідомлення на застосунок у телефоні. За допомогою інтегрованого динаміку та мікрофону можливий двосторонній зв’язок. Є підтримка флеш-пам’яті формату microSD максимальним об'ємом до 128 ГБ.
- IP камера Dahua DH-IPC-HDW2230– цифрова камера із 2МП розподільчої здатності. Має вбудовану інфрачервону підсвітку для нічної зйомки. Може встановлюватися ззовні приміщень і всередині них. Камера має конструкцію «Eyeball», металічний корпус із пластиковим кріпленням. Інтерфейси є роз’єм живлення 12В та мережевий вхід із підтримкою Power on Lan.

- Гібридна камера AHD Green Vision GV-112 – дана камера має високу розподільчу здатність 5МП. ЇЇ головною особливістю є можливість працювати як за допомогою аналогового інтерфейсу так і цифрового. За допомогою аналогового коаксіального кабелю дальність передачі можлива до 500 метрів. В іншому випадку можна використати Ethernet кабель типу «вита пара». Дана камера також підтримує інфрачервоне підсвічування. Має матрицю типу CMOS;
- IP-відеокамера 4Mpx Dahua IPC-K42P IMOU Cube – цифрова камера яка оснащена 4МП матрицею із можливим фокусним відстанню 2.8 мм, можливість інфрачервоного підсвічення до 10 метрів. Вбудований інфрачервоний датчик для виявлення руху об'єктів, також можлива двох сторонній зв'язок за допомогою інтегрованих мікрофона та динаміку
- Гібридна Камера HAC-TA21P – цифрова 2 МП камера купольної конструкції. Фокусна відстань 2.6 ммЄ, кут огляду становить 93 градуси. Підтримує інтеграцію із платформою IMOU, Інфрачервоне підсвічування дозволяє вести нагляд за територією до 20 метрів, підтримка microSD флеш–пам'яті. Підтримує дальність передачі 300 м по UTP та 800 м по коаксіальному кабелю. Може передавати одразу декілька сигналів по кабелю: керуючий, відеопотік та звуковий сигнал.
- Відеокамера EZVIZ CS-C6N – поворотна купольна камера роздільної здатності 2 МП. Додаткова можливість автостеження за об'єктом. За дпомогою своєї конструкції може знімати у режимі панорами, що забезпечує огляд усього приміщення при куті огляду 340 градусів. Можливо включити режими у якому камера автоматично виявлятиме рух, направлятиметься на нього та починатиме зйомку відео із подальшим відправленням отриманого матеріалу на головний пульт охорони системи безпеки. Камера має вбудований модуль Wi-Fi, що дозволяє підключити її безпроводовим способом.

Для даного проєкту було обрано камеру Dahua IPC-K42P IMOU Cube 4MP (рис. 2.7) оскільки вона має можливість інтеграції із системою Ajax Systems та високу чіткість зображення 2560 x 1440 та його добру стиснення даних відеокодеком H.265, що є гарними характеристиками як для своєї ціни.

Рисунок 2.7 – Обрана відеокамера

Приведемо список асортименту відеореєстраторів для системи відеонагляду:

- Hikvision DS-7616NI-Q1 – мережевий реєстратор із підтримкою до 16 камер, максимальний вхідний потік даних 160 Мбіт/с. Сумісний із популярними кодеками стиснення даних: H.265/H.265. Також наявні два USB порти. відноситься до обладнання професійного класу. Підтримка жорсткого диску до 6 ТБ підключеного через SATA інтерфейс.
- Hikvision DS-7104NI-Q1/4P – чотирьох канальний мережевий відео-реєстратор для IP камер до 4 штук. Підтримує живлення типу PoE до 36 Вт. Максимальна потокова швидкість складає 40 Мбіт/с. Підтримка пам'яті до 6 ТБ. Роздільна здатність камер до 4 МП у 1080p якості.
- Dahua DHI-NVR2116-I – мережевий відеореєстратор із підтримкою до 16 цифрових камер. Має зручний веб інтерфейс для налаштування камер. Підтримує технології розпізнавання обличь, які знаходяться у внутрішній базі даних. Максимальна підтримувана якість відео 4K роздільної здатності, жорсткий диск до 6 ТБ.
- CoVi Security NVR-4500 – мережевий відеореєстратор який дозволяє обробляти 8 камер, максимальна роздільна здатність 4K. Підтримка до 8 ГБ жорсткого диску. Наявні 3 USB порти.

Для побудови системи безпеки на підприємстві було обрано відеореєстратор моделі Dahua DHI-NVR2116-I. Оскільки він має зручний інтерфейс, що полегшує налаштування та подальших супровід обладнання та сумісний із відео обладнанням там контролером безпеки.

2.3.6 Мережеві брандмауери

Мережевий екран – це програмний або програмно-апаратний продукт, призначення якого відстежувати мережевий трафік на рівні пакетів та в залежності від їх змісту дозволяючи чи відхиляючи їхнє проходження. Таким чином забезпечується захист серверів, клієнтів та корпоративних служб від несанкціонованого доступу. Також цей інструмент називають firewall або брандмауером[10, 17].

Приведемо список асортименту мережевих екранів:

- FG-100E Fortinet – мережевий екран серії FortiGate для забезпечення безпеки офісних мереж корпоративного типу. Пропускна здатність приладу близько 7,4 Гбіт/с він обладнананий 20 портами RJ-45 із швидкістю 1GbE, два з яких виконують роль WAN роз'ємів. Також є два комбінованих входи з гігабітними SFP роз'ємами. Також є один USB роз’єм. FG-100E підтримує технології IPsec VPN, SLL VPN і блико 10 тисяч VPN тунелів.
- Fortinet FWF-30E – є продуктивним мережевим екраном з вбудованою бездротовою точкою доступу стандарту 802.11n. Ця модель може комутувати чотири гігабітні порти один із яких виконує роль WAN. Особливістю даного екрану є 16 ГБ внутрішнього сховища. Максимально можлива пропускна спроможність є на рівні 950 Мбіт/с. Підтримується VPN на 250 тунелів. Такий мережевий екран підходить для забезпечення захисту невеликих локальних офісних мереж.
- Ubiquiti UniFi Security Gateway – поєднує розширені функції безпеки з потужною технологією маршрутизації. Має один WAN порт та один LAN, і ще один порт має гібридну конфігурацію Швидкість обробки даних 3 Гбіт/с

Цей мережевий екран здатний маршрутизувати до 1 мільйона пакетів за секунду.

- Cisco ASA5506-K8 – цей мережевий екран включає в себе контроль і детальний моніторинг мережі, надійний багаторівневий захист, систему запобігання вторгненням IPS, комплексний захист від шкідливого ПЗ, Cisco AnyConnect для віддаленого доступу та багато іншого. Швидкість обробки інформації 750 Мбіт/с [15].
- ZYXEL USG20 – розроблений спеціально для забезпечення надійного та безперервного сервісу VPN, який також підтримує подвійний WAN для забезпечення дублювання провайдера. У пристрої задіяні 2 з'єднання WAN, один є основним, а другий резервним. І якщо трапиться збій, тоді Zyxel VPN Firewall в автоматичному режимі одразу ж приєднається до резервного. І як тільки основний буде відновлено, одразу ж буде зворотне підключення до нього. Пропускна здатність 90 Мбіт/с.
- D-Link DFL-870 – даний міжмережевий екран підтримує розширенні функції повідомлення користувачів за допомогою внутрішньої системи оповіщення. Також підтримує систему виявлення та затримки вторгнень UTM. Можливо керувати політиками застосунків. Підтримує популярні VPN протоколи PPTP, IPSec, , L2TP та SSL4. Має 2 USB порта та 6 1Гбітних портів.

Рисунок 2.8 – Обраний мережевий брандмауер

З огляду на вищеописані пристрої було прийнято рішення в якості мережевого екрану для підприємства вибрати 3xGE Ubiquiti UniFi Security Gateway, оскільки він має гарне співвідношення ціна та продуктивність та зручне для налаштування програмне забезпечення.

2.3.7 Протипожежні датчики

Пожежна сигналізація – це система сповіщувачів, виконавчих механізмів та інших засобів для швидкого виявлення та оповіщення про займання вогню на об'єкті із подальшою відправкою керуючих сигналів для систем оповіщення про пожежу та автоматичного пожежогасіння [3].

Приведемо список асортименту обладнання для протипожежного захисту:

- FireProtect Ajax – безпроводовий датчик виявлення пожежі із вбудованим сенсором температури [11]. Може виявляти задимлення за допомогою камери з фотоелектричним датчиком. В разі якщо під час займання відсутній дим є додатковий датчик який може виявити різке підвищення температури у приміщенні. Поріг спрацьовування +59°C.
- CV-212-12-01 – автономний пожежний датчик, який є частиною пожежної сигналізації. Має внутрішню будову оптоелектронного детектора , що дозволяє встановлювати його у приміщеннях із агресивними середовищами. Даний сповіщувач має сирену та світлову індикацію при виявленні перевищення певного рівня задимленості в приміщенні, що охороняється.
- FireProtect Plus – покращений варіант базової версії, відмінністю є датчики не лише температури та задимленості, а і сенсор чадного газу, що у купі із безпроводовими можилвостями пожежний сенсору дозволяє провести цілодобовий моніторинг за безпекою у приміщенні та швидко оповіщати про можливість пожежі, задимленості чи чадного газу

Рисунок 2.9 – Обраний протипожежний сповіщувач

Було обрано FireProtect Ajax, оскільки він має інтеграцію із системою контролю охоронної мережі, легке встановлення, налаштування та гібридну модель виявлення пожежі чи задимленості у приміщенні.

2.3.8 Кінцеві прилади

Кінцеві прилади – в загальному випадку це усі ті пристрої охоронної системи із якими стикається звичайний користувач у повсякденному користуванні. Це можуть бути різноманітні панелі керування, світлові індикатори та монітори. За допомогою них можна користуватися охоронною мережею, наприклад ставити її на охоронний режим чи вимикати цей режим.

Для керування та індикації подій із кінцевих приладів для проекту системи безпеки доцільно розглянути клавіатури введення та сирени. Оскільки вже обраний контролер екосистеми Ajax, тому потрібно обрати сумісні із ним кінцеві прилади перерахуємо обрані компоненти системи безпеки[13]:

- KeyPad Jeweller – сенсорна клавіатура введення із без проводовим інтерфейсом. ЇЇ основною функцією є зняття чи встановлення стану режиму охорони об’єкту. Режим охорони можна зручно включити натисканням однієї клавіші Передбачається, що дана сенсорна палень буде встановлена біля вхідних дверей. На індикаторній панелі показується статус з’єднання із головним контролером, статус сповіщувачів та охорони в цілому. Підтримує до 99 кодів доступу які налаштовується через центральний контролер.
- HomeSiren Jeweller – сирена для приміщення із бездротовим підключенням. Головне призначення гучно сигналити при сигналі тривоги. Видає звуковий сигнал при зміні режимів системи охорони. Можливо підключити зовнішню світлову індикацію. У конфігурації можливо налаштувати рівень гучності та часу звукового сигналу.

2.3.9 Додаткове обладнання

Для побудови системи безпеки необхідно додаткове обладнання опишемо його [13]:

Для стабільного зв'язку в умовах міської забудови та інтенсивного обміну трафіку через бездротові мережі, доцільно обрати ретранслятор зв'язку, для забезпечення стабільності роботи без проводових сповішувачів та усієї мережі в цілому. Ajax ReX 2 – це ретранслятор радіосигналу по протоколу Jeweller, він дозволяє розширити площу зони, що охороняється. Окрім цього забезпечити надійний зв'язок у тих місцях де відбуваються перебої із радіозв'язком за рахунок проводового підключення до головного контролеру. За допомогою нього можна будувати систему безпеки із більшою гнучкістю, розміщаючи датчики саме там де вони потрібні – не залежно від статусу радіо з'єднання. Максимальний ліміт таких ретрансляторів у одній системі 5 штук. Ретранслятор має 4 антени та підтримку двох протоколів Jeweller для відправки команд керування, подій та Wings для потокової передачі фотознімків. Обидва протоколи підтримують шифрування та автентифікацію для захисту від злому.

ВИСНОВОК

У другому розділі було описано загальну структуру підприємства із картою його офісної будівлі, окрім цього було проведено огляд стану комп'ютерної мережі підприємства із переліком обладнання що є у ньому.

Був проведений опис майбутнього проєкту системи безпеки із рядом вимог фізичної, інформаційної та пожежної безпеки, що повинні виконуватися для цього підприємства.

У останній частині розділу був проведений аналіз сучасного асортименту обладнання для побудови системи безпеки таке як: контролери для мережі, датчики руху, розбиття скла, відкриття дверей, системи відеоспостереження, мережеві екрани, протипожежний захист та інше додаткове обладнання.

3 ВПРОВАДЖЕННЯ ОХОРОННОЇ СИСТЕМИ ІЗ КОНТРОЛЕМ ДОСТУПУ НА ПІДПРИЄМСТВІ

3.1 Визначення розташування компонентів системи безпеки та їх монтаж

3.1.1 Визначення об’єктів охорони на підприємстві

Об’єктом охорони у комерційному підприємстві є ті прилади чи устаткування які потребують захисту чи контролю доступу, для ефективного монтажу компонентів системи безпеки, потрібно визначити місцезнаходження об’єктів охорони.

Зазначимо на карті підприємства (рис 3.1) основні об’єкти охорони, у подальшому ці позначення допоможуть орієнтуватися із місцезнаходженням компонентів системи безпеки у наступних підрозділах де буде безпосередньо визначено місце їх монтажу.

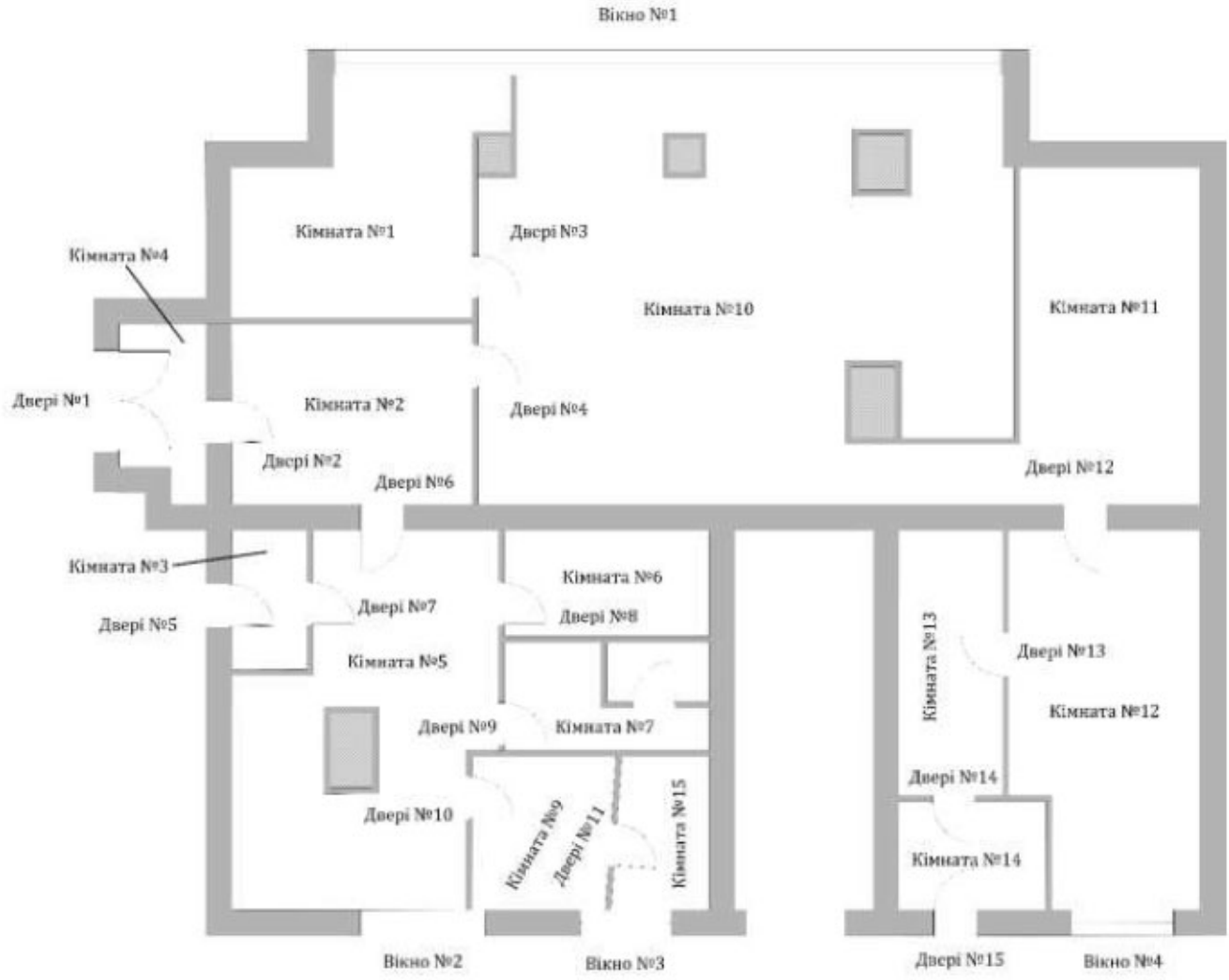


Рисунок 3.1 – Позначення об’єктів охорони на підприємстві

Опишемо кімнати як об’єкти охорони та контролю доступу (табл. 3.1).

Таблиця 3.1 – Опис об’єктів охорони на підприємстві

Об’єкт охорони	Опис
Кімната №4	Головний вхід у підприємство.
Кімната №3	Додатковий вхід у підприємство.
Кімната №1	Робоче місце, 1 ПК і 1 принтер
Кімната №2	Тамбур
Кімната №5	Хол
Кімната №6,7,13,15	Приміщення вторинного значення
Кімната №10	Робоче місце: 6 ПК, 2 принтери, Wi-Fi точка.
Кімната №11	Серверна: сервер, файлове сховище, мережеве обладнання, 6 ПК
Кімната №12	Робоче місце: 5 ПК
Кімната №14	Додатковий вхід у підприємство

Пріоритетними зонами для охорони у підприємстві є кімнати із розташованими робочими місцями та мережевим обладнанням таким як сервер та файлове сховище і комунікаційне приладдя. Серверна має найбільший пріоритет захисту оскільки в разі правопорушення в даному випадку підприємство понесе не лише матеріальні збитки із за непрацездатності обладнання, а й що важливіше – репутаційні втрати, оскільки на сервері та NAS знаходяться важливі конфіденціальні дані клієнтів підприємства, втрата чи розповсюдження яких є не припустимою.

3.1.2 Монтаж датчиків руху

Для організації системи захисту в приміщеннях, а саме захисту від фізичного проникнення, класичним рішенням є – контроль присутності людини за допомогою датчиків руху. Їх потрібно встановлювати у місцях найбільшої вірогідності знаходження людини та там де потрібно контролювати їх не бажану присутність, наприклад присутність руху на складському приміщенні у не робочі часи зазвичай є ознакою правопорушення що до підприємства. Окрім цього датчики руху можуть

запускати різноманітні сценарії працюючи сумісно із контролером охоронної мережі, наприклад запуск сирени та світлового сповіщення.

У проекті модернізації системи безпеки підприємства використовуються датчики виявлення руху моделі Ajax MotionProtect. Цей датчик має бездротовий інтерфейс підключення тобто не потребує додаткового монтажу кабелів. Він працює за принципом пасивного інфрачервоного випромінювання, із за чого його доцільним місцем розташування є верхня частина стіні під стелею на висоті близько 2.4 м, передньою стороною до зони, що необхідно контролювати. Цей датчик руху підключається за допомогою мобільного застосунку (за допомогою QR коду) до центрального хабу (контролеру) охоронної мережі. Він має автоматичне регулювання чутливості із трьома ступенями. Фізично сенсор монтуєтеся на кріплення SmartBracket. Слід зазначити не миттєвий час переходу датчику на режим охорони, за замовчуванням він складає 36 с. Після встановлення датчику за допомогою застосунку доцільно запустити тестування рівню сигналу та зони сповіщення.

Опишемо обладнання датчиків руху, що необхідно змонтувати із зазначенням кімнат та його призначення:

- Стіна навпроти двері у кімнату №1, тут розташоване важливе робоче місце тому тут потрібно виявлення небажаних відвідувачів.
- Більшу частину кімнати №10 охоплює робоча зона датчику №2. Тут розташовано багато робочих місць та обладнання, тому захист цього приміщення є важливим.
- Датчик №3 у кутку приміщення кімнати №11. Тут фізично розташована мережеве обладнання включаючи сервер та файлове сховище, охорона цього обладнання є пріоритетним для підприємства.
- Сенсор руху №5 охоплює зону можливого проникнення через додатковий вхід.
- У кімнаті №12 встановлений датчик руху №4, його місцерозташування обумовлене наявністю робочих місць із персональними комп'ютерами які потрібно охороняти.

Відобразимо точки монтажу датчиків руху на мапі підприємства (рис. 3.2)

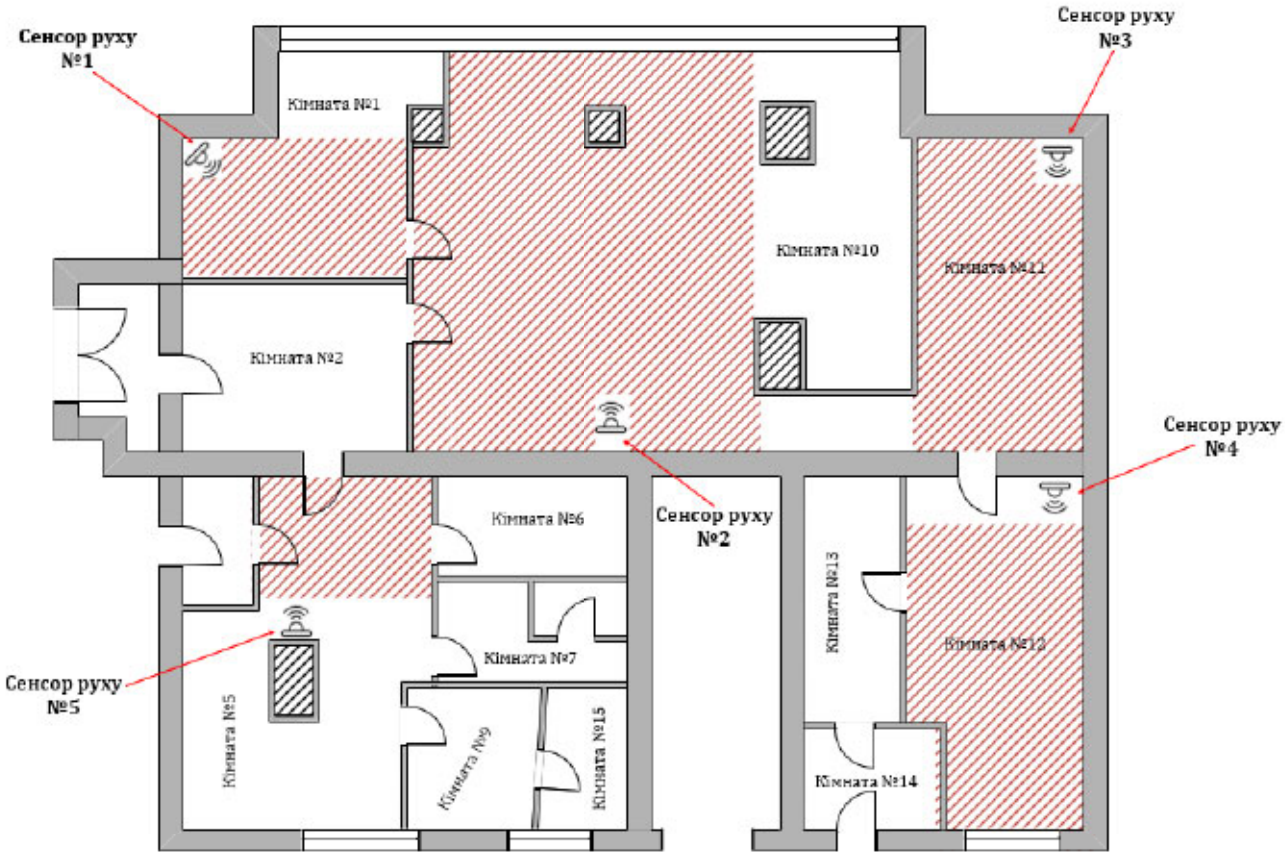


Рисунок 3.2 – Позначення точок встановлення датчиків руху

3.1.3 Монтаж датчиків відкриття дверей

Датчики відкриття дверей складаються із двох компонентів магніту та сенсору, шо реагує на магнітне поле. Зазвичай датчик встановлюється на дверну раму, а магніт закріпляється на дверях. При закритих дверях магніт та датчик повинні бути один навпроти одного із невеликим зазором.

Принцип дії такої системи в тому що коли двері відчиняються магніт разом із дверями віддаляється від датчику та він перестає уловлювати магнітне поле, це і свідчить про стан дверей – відкрити чи закриті.

У ролі датчиків відкриття дверей використовуються сенсори Ajax DoorProtect, вони не потребують проводового з'єднання. Складається із двох компонентів, сенсору та окремого магніту. Магніти є двох різновидів в залежності від товщини потрібної товщини зазору,

Опишемо обладнання датчиків відкриття дверей, що необхідно змонтувати із зазначенням кімнат та його призначення:

- Датчик відкриття дверей у кімнаті №1, забезпечує захист від проникнення головних офісних дверей.
- Датчики №2 та №3 слідкують за станом додаткових виходів на підприємстві

Відобразимо точки монтажу датчиків відкриття дверей на мапі підприємства (рис. 3.3)

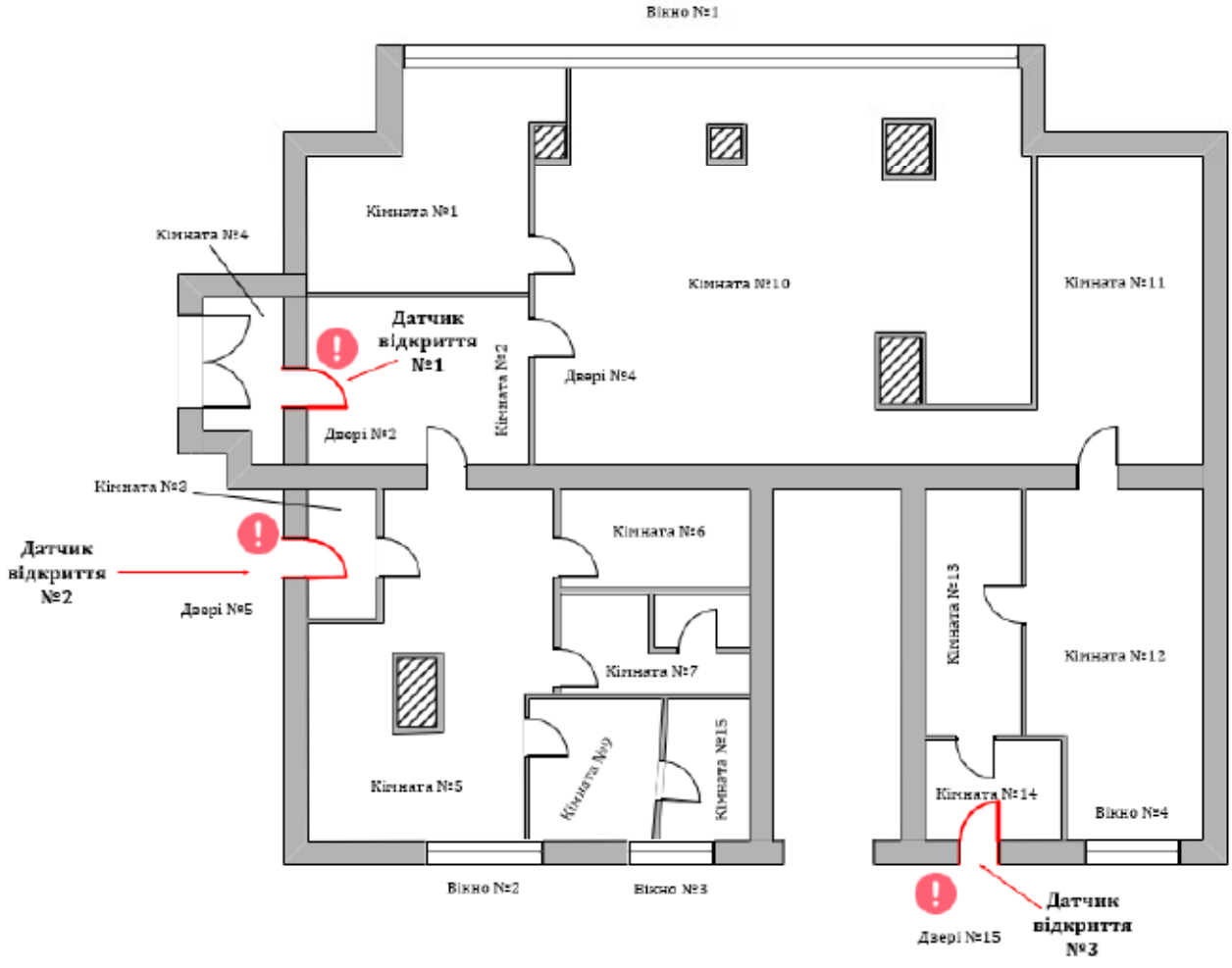


Рисунок 3.3 – Позначення точок встановлення датчиків відкриття дверей

3.1.4 Монтаж датчиків розбиття скла

Датчики розбиття скла запрограмовані на визначення певної частоти звуку розбитого скла. Вони повинні бути встановлені в межах десятка метрів від вікон, які потрібно захистити.

Для захисту вікон на підприємстві вирішено використовувати модель датчику розбиття скла Ajax GlassProtect. Він працює по бездротовому інтерфейсу у Jeweller. Датчик потрібно встановлювати у межах 9 метрів від вікна. Загалом цей датчик має легкий процес встановлення і не потребує навіть початкового налаштування, але за необхідності можна встановити конфігурацію через мобільний застосунок.

Опишемо обладнання датчиків розбиття скла, що необхідно змонтувати із зазначенням кімнат та його призначення:

- Датчик №1 встановлюється на головне велике вікно, яке виходить у хол та кімнату №1, дане вікно є потенційним вектором атаки зловмисника тому доцільно його захищати.
- Усі інші вікна також захищені датчиками розбиття скла №2,3 та 4. Такий підхід дозволяє зменшити вірогідність порушення зони контролю до мінімуму.

Рисунок 3.4 – Позначення точок встановлення датчиків розбиття скла

3.1.5 Монтаж обладнання відеоспостереження спостереження

Працююча система відеоспостереження, може забезпечити цілодобове повне покриття території. Камери відеоспостереження знімають все, що відбувається на об'єкті та навколо нього, а потім надсилають кадри на реєстратори, монітори чи мобільні пристрої.

Для відеоспостереження обрано модель відеокамери Mpx Dahua IPC-K42P. Ця камера розрахована на монтаж усередині приміщень, вона працює по протоколу Wi-Fi та може інтегруватися із системою Ajax як додатковий сенсор у охоронній мережі. Також камера має вбудований сенсор виявлення руху.

Для налаштування камери достатньо сканувати QR код мобільним застосунком для інтеграції у систему Ajax, через дану систему можливий перегляд у режимі реального часу. Камера підтримує налаштування режимів виявлення руху, тривоги, архівування та запису навколишнього звуку. При налаштування слід враховувати кут огляду відеокамери у 97°, також те що камера дозволяє знімати у повній темряві за рахунок інфрачервоного підсвічування, його дальність складає до 10 метрів. У камери є власний кронштейн що дозволяє з легкістю її змонтувати на більшість поверхонь.

Для підключення комплекту системи відеоспостереження потрібно:

- IP камери,
- відеореєстратор,
- жорсткий диск для запису та зберігання відео матеріалів,

Опишемо обладнання відеоспостереження, що необхідно змонтувати із зазначенням кімнат та його призначення:

- Усього на підприємстві було встановлено чотири відеокамери.
- Камера №1 споглядає за головним входом, фіксуючи на відео усе що відбувається коло них.
- Відеокамери №4 та №2 слідкують за станом приміщень у робочих кімнатах, також. Їх присутність дозволяє гарантувати запис на відео правопорушень у цих кімнатах із великою кількістю обладнання та працюючого персоналу.

- Відеокамера №3 встановлена у серверній, кімнаті де розміщено одне із найважливіших обладнань на підприємстві – сервер, NAS. Розміщення тут відеокамери є обов'язковим рішенням.

Рисунок 3.5– Позначення точок встановлення камер відеоспостереження

3.1.5 Монтаж протипожежних датчиків

Протипожежні сповіщувачі встановлюються зазвичай десь на стелі або на стіні під нею, вони можуть виявляти пожежу за допомогою виявлення високої температури або задимлення або високої концентрації якогось газу.

Для захисту від пожеж на підприємстві встановлено протипожежні сповіщувачі моделі FireProtect Ajax, цей датчик підтримує бездротове підключення, принцип є гібридним: фіксує задимлення в приміщені та підвищення температури. Може працювати у автономному режимі без з'єднання із

центральним контролером охоронної мережі. Для розширеного налаштування можна підключити до контролера за допомогою застосунку, сам датчик має кріплення типу SmartBracket.

Опишемо обладнання датчиків руху, що необхідно змонтувати із зазначенням кімнат та його призначення: протипожежні датчики встановлені в великих приміщеннях, що б мати змогу ефективно та швидко виявляти та попереджати пожежі на підприємстві. Через інтеграцію із центральним хабом вони можуть вмикати головну сирену на підприємстві.

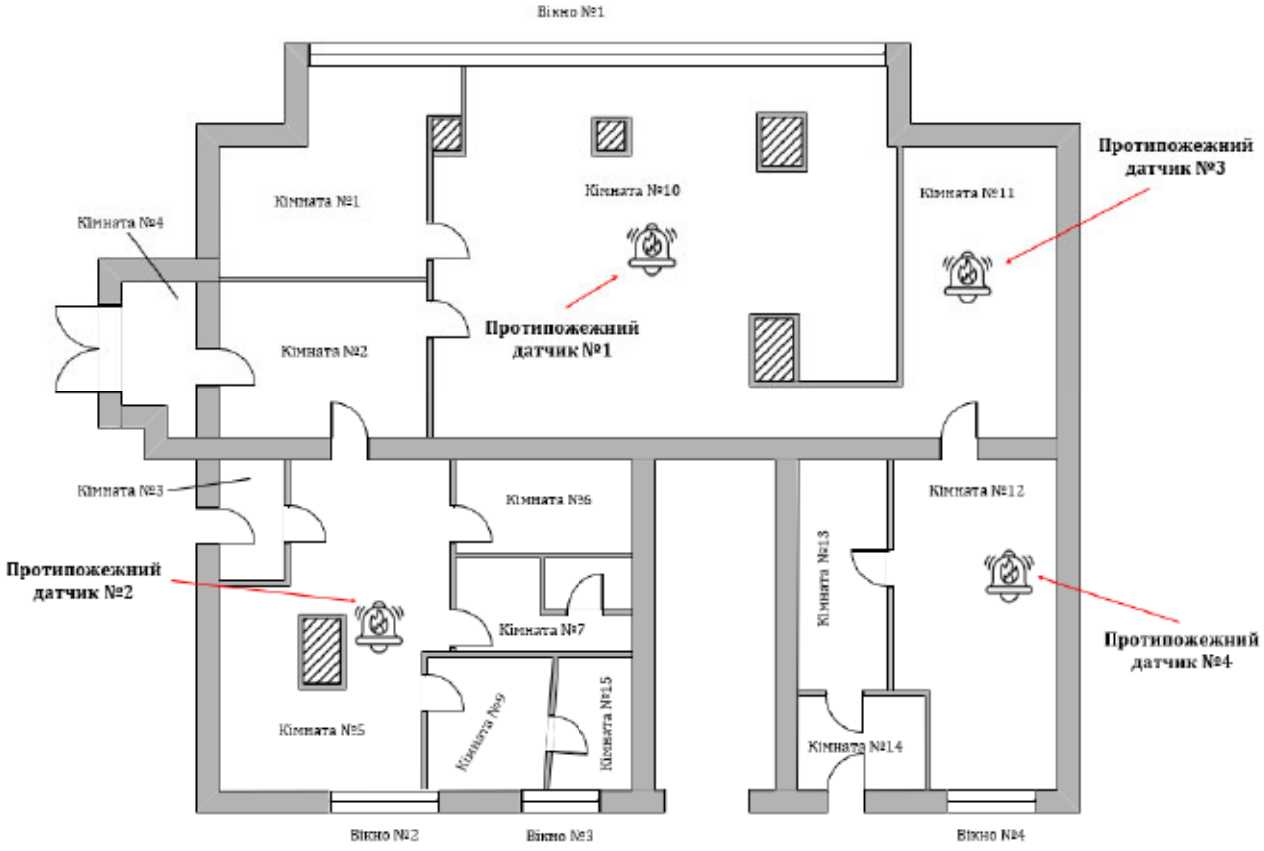


Рисунок 3.6 – Позначення точок встановлення протипожежних датчиків

3.1.6 Монтаж кінцевого обладнання

Один із кінцевих обладнань є клавіатури для введення різноманітної інформації від користувачів. Але найчастіше її використання це постановка системи на охорону та зняття з неї, тобто це консолі доступу до приміщень офісного будинку де розташоване підприємство.

В ролі клавіатури введення обрана сенсорна бездротова клавіатура Ajax KeyPad. Вона дозволяє при введені коду чи натисканні кнопки посилати радіосигнал на центральний контролер для включення чи відключення охорони, крім того вона має вбудований RFID зчитувач, що є зручним способом авторизації для персоналу.

Опишемо додаткове обладнання, яке необхідно змонтувати із зазначенням кімнат та його призначення:

- Сирена сповіщення встановлена у центральному холі, для звукової індикації про надзвичайні події.
- Клавіатури введення є біля кожного входу у підприємство для контролю доступу дверей та зняття та постановку на охорону усієї будівлі.

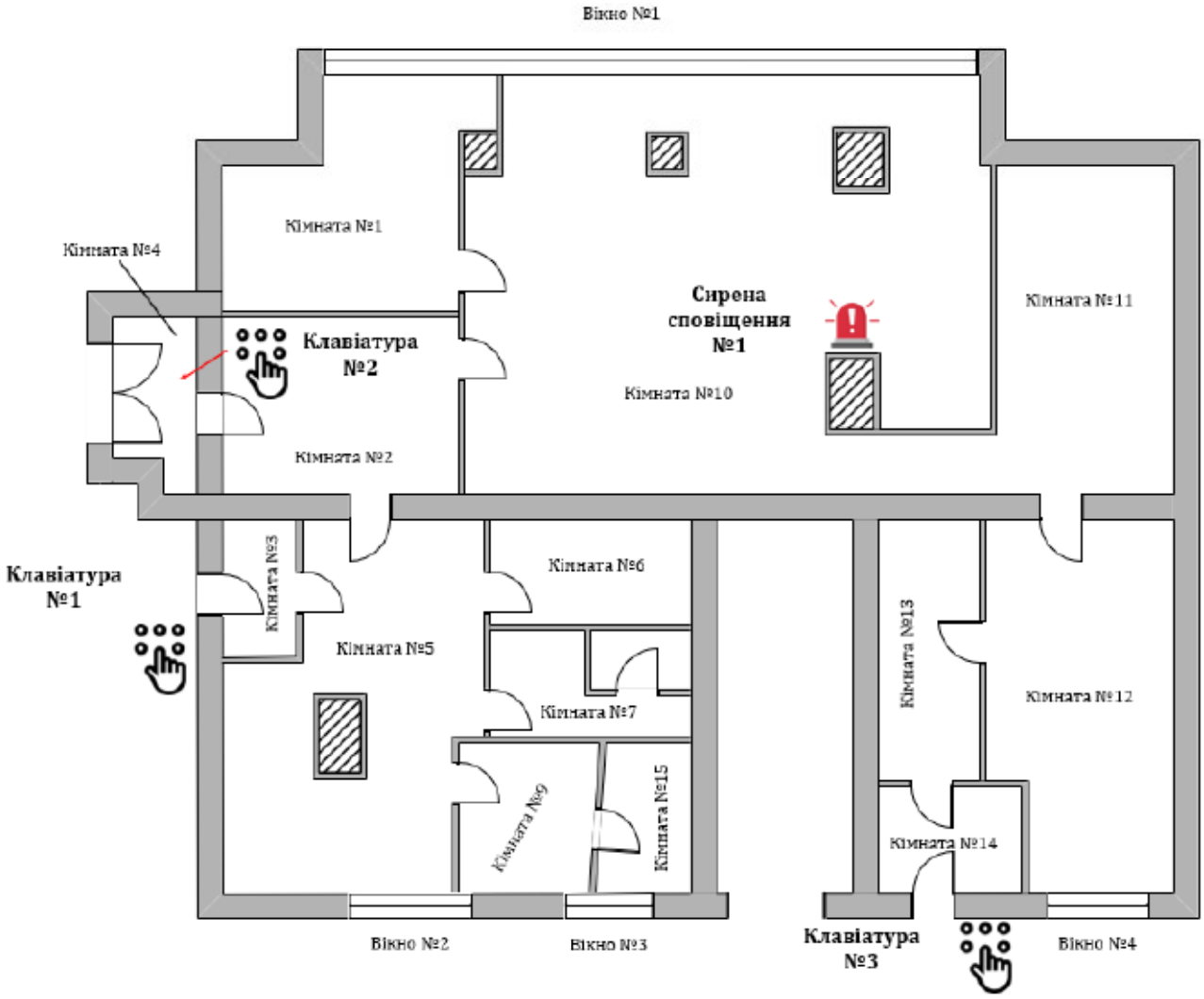


Рисунок 3.7– Позначення точок встановлення кінцевого обладнання

3.1.7 Монтаж додаткового обладнання

Для зменшення впливу завад та гарантованого зв'язку на підприємстві доцільно розташувати ретранслятор сигналу такий як Ajax ReX 2. Він має підтримку таких бездротових протоколів як: Jeweller та Wings. Перший передає команди, події та сигнали тривоги, а другий надає можливість передавати фото знімки. Використання кадрів для синхронізації сеансу зв'язку дозволяє реалізувати двох сторонній бездротових зв'язок через радіоканал, що дозволяє проводити автентифікацію, шифрування та захищати канал зв'язку від будь-якого зловмисного втручання та витоку персональних даних. Можна реалізувати альтернативний запасний варіант зв'язку в разі відсутності доступу до бездротового інтерфейсу через локальну мережу підприємства використовуючи мережевий порт Ethernet.

Ретранслятор встановлений у протилежній центральному контролеру частинці офісу для подовження радіусу охоплення бездротового зв'язку системи безпеки на підприємстві.

Рисунок 3.7 – Позначення місця встановлення додаткового обладнання

3.1.8 Монтаж контролеру охоронної мережі

Контролер охоронної мережі є головним елементом для управління та контролю іншими компонентами системи безпеки на підприємстві. Контролер збирає інформації від усіх сповіщувачів, обробляє ці дані та в разі чого запускає різні сценарії реагування на події.

У ролі центрального хабу, тобто контролера для охоронної мережі підприємства було обрано Ajax Hub 2 Plus він підтримує GSM та Ethernet технології. Налаштування усієї екосистеми датчиків Ajax та деяких сторонніх апаратних засобів. Його встановлення підтримує кріплення типу SmartBracket.

Фізично контролер розташований у серверній кімнаті разом із іншим мережевим та комутаційним обладнанням.

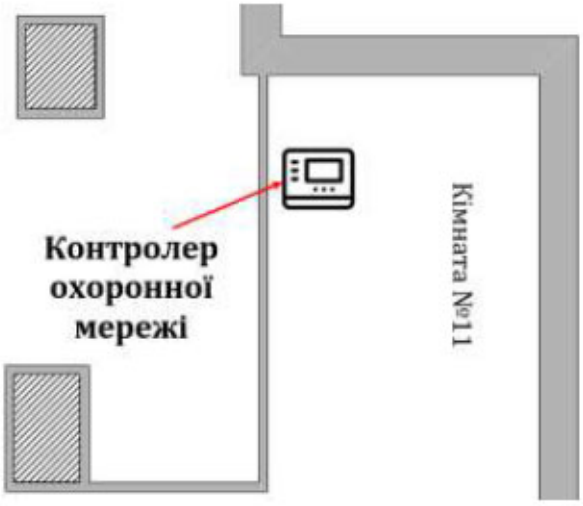


Рисунок 3.8 – Позначення місця встановлення контролеру охоронної мережі

3.2 Інтеграція системи безпеки із мережею підприємства

3.2.1 Контролер системи безпеки

Для інтеграції із мережею підприємства контролер охоронної мережі використовує Ajax Cloud через проводове з'єднання Ethernet або GSM мережу оператора стільникового зв'язку.

Контролер головний мережі потребує постій доступ до глобальної мережі Ethernet, що б підключатися до хмарного сервісу Ajax Cloud – за допомогою нього проводиться конфігурація та управління контролеру, моніторинг стану об'єктів, оновлення програмного забезпечення для сповішувачів та іншого обладнання. Окрім цього збираються архівні дані (лог) для подальшого аналізу роботи та працездатності охоронної мережі та легшого виявлення несправностей у ній.

Обмін даними із хмарним сервісом відбувається у шифрованому вигляді із автентифікацією користувачів, таким чином забезпечується захист персональних даних та всієї мережі в цілому.

Максимальний ліміт одночасно приєднаних до контролеру пристроїв складає 100 Ajax приладів. Бездротовий зв'язок із іншими пристроями у мережі реалізується через Jeweller із максимальним радіусом дії до 2 км, за відсутності шумів чи інших перешкод.

Контролер дозволяє налаштувати такі мережеві параметри у своєму меню конфігурації:

- Ethernet – керування станом готовності Ethernet у контролері.
- DHCP чи Static – динамічна видача мережевих адрес, чи ручні налаштування окремо для кожного пристрою.
- IP-address – мережева адреса контролера.
- Маска підмережі – бітова маска що задає робочу підмережу для контролера.
- Шлюз – маршрутизатор через який буде йти трафік у глобальну мережу.
- DNS – налаштування серверу доменних імен для контролера.

3.2.2 Системи відеоспостереження

У Ajax Systems дозволяє інтеграцію цифрових IP-камер від сторонніх виробників, інтегруючи прямо в інтерфейс програми налаштування AJAX.

Для того щоб перевірити сумісність камери із системою AJAX потрібно перевірити підтримку її протоколів на сайті виробництва. Потрібна підтримка протоколу реального часу – RSTP. Такий протокол сумісний із обладнанням AJAX та буде правильно працювати із його програмним забезпеченням, адже лише такий формат потокових даних розуміє програма налаштувань Ajax.

Для автоматичного налаштування мережевих портів, бажана, але не обов'язкова підтримка технології UPnP, за допомогою неї камера зможе автоматично налаштуватися, без необхідності ручного додавання мережевих правил на маршрутизаторі чи мережевому екрані.

Для підключення камер до відеорегістратору потрібно що б кожна камера і реєстратор повинні мати різні IP адреси, але підмережі однакові. Якщо є кілька відеокамер, підключення до реєстратора здійснюється через комутатор або роутер. Опишемо порядок підключення відеокамери до реестратору:

- Має бути повністю налаштований відеореєстратор із підключеним монітором, мишею та встановленим жорстким диском, для запису архівів відео локально.
- Потрібно підключити камеру безпосередньо до реєстратора або через комутатор.
- Натисніть кнопку «Додати IP-камеру». У реєстраторах різних виробників цей пункт позначений по-різному, англійською ця кнопка називається add IP-camera.
- Після цього пристрій виконає пошук усіх камер у мережі, і буде функція додати камери до списку взаємодії. Далі з'явиться доступ до налаштувань камер. Щоб підключити IP-камеру до відеореєстратора, потрібно змінити IP-адреси, щоб останній блок був унікальним для кожної камери, і встановити їм однакові з реєстратором паролі.
- Також можна вибрати параметри запису та інші параметри в меню реєстратора. Задати йому зовнішню IP-адресу можна через меню маршрутизатору.

3.2.3 Налаштування мережевого брандмауера

На підприємстві встановлений мережевий брандмауер Ubiquiti Unifi Security Gateway. За допомогою нього можливо не лише контролювати мережевий трафік, а ще і збирати статистику для покращення якості роботи мережі.

Опишемо його налаштування для коректної роботи та захисту мережі підприємства:

- Для коректного налаштування необхідно встановити на робочий ПК, що під'єднаний до тієї локальної мережі, що і мережевий екран, програму UniFi Controller [18]. Замість нього також можна використовувати апаратний засіб Ubiquiti Unifi Cloud Key, але для маленького підприємства це надмірно.
- До першого WAN порту необхідно підключити кабель інтернет провайдеру, у інший порт підключається комутатор, що з'єднує локальну мережу підприємства.
- У запущеній програмі налаштування UniFi Controller повинен з'явитится статус мережевого екрану.
- Натиском кнопки «Adopt» на ньому можна добавити його до мережевої інфраструктури. За можливості на даному етапі може з'явися повідомлення про необхідність оновлення внутрішнього програмного забезпечення мережевого екрану.
- Для доступу у меню налаштувань необхідно натиснути кнопку «Configuration».
- У головній секції екрану конфігурації можна налаштувати режим підключення до зовнішньої мережі: динамічний IP, статичний IP, PPPoE та інші параметри такі як: ім'я приладу, тип з'єднання.
- Тип підключення до зовнішньої мережі потрібно поставити – динамічний IP, для автоматичного налаштування від інтернет провайдеру, оскільки провайдер на підприємстві підтримує таку функцію.
- Тип з'єднання для локальних пристроїв – DHCP для автоматичної видачі мережевих адресів з'єднаним пристроям.
- За необхідності окремо можливо налаштувати DNS сервери та VLAN.
- Після усіх необхідних налаштувань натиснути кнопку Queue Changes.

Для роботи підприємства може знадобитися функція публікації ресурсів локальної мережі у зовнішню мережу, так зване «прокидування портів» або port forwarding. Опишемо процес налаштувань відкриття портів на мережевому екрані:

- Необхідно зайти у програму налаштувань UniFi Controller.
- Обрати вкладку «Configuration», а там вибрати меню «Port Forward».

- Відкриєтеся меню де можна задати мережеве правило у якому потрібно вказати назву, внутрішній (локальний) адрес пристрою, внутрішній порт, та зовнішній порт. Та натиснути кнопку прийняти конфігурацію.
- За допомогою такої функції можна зв'язувати довільні зовнішні порти на мережевому екрані із внутрішніми портами локальних пристроїв у мережі.

У програмі налаштувань у вкладці «Networks», можна налаштувати роботу різних типів мереж (VLAN). Використання такої функції дозволяє віртуально ізолювати трафік мереж один від одної, передаючи його по одному і тому ж апаратному середовищу.

Опишемо процес налаштування VLAN на мережевому екрані:

- У вкладці «Network» необхідно обрати мережу за замовчуванням. Це необхідно для того, що б усі промарковані VLAN пакети будуть йти через відповідну їм мережу, а увесь не промаркований трафік у мережу за замовчуванням.
- Вкладка «Services» дозволяє налаштувати параметри такі як керуючий VLAN, підтримку великих (Jumbo) пакетів. Можливо також налаштувати швидкість потоку даних через чекбокс «Flow control».

Для швидкого моніторингу стану мережі можна використовувати першу сторінку стану мережі «Network health» Він показує графіки уявлення про стан мережі. Базова інформація надається для кожної складової. Колір індикаторів відповідає наступним станам мережі:

- Зелений індикатор – усі пристрої функціонують нормально.
- Помаранчевий – застосовується тільки для бездротової мережі і означає, що кілька (менше половини) точок доступу відключені від мережі.
- Червоний – означає відсутність інтернет з'єднання.

Даний мережевий екран підтримує технологію DPI (Deep Packet Inspection), що дозволяє проводити детальну інспекцію пакетів, що проходять повз мережевий екран таким чином збираючи детальну статистику того який саме трафік проходить у мережі підприємства та яким чином його використовують користувачі.

3.5 Розрахунок вартості системи безпеки

3.4.1 Підрахунок необхідної кількості обладнання

Для розрахунку вартості всієї системи безпеки необхідно порахувати кількість одиниць обладнання кожного типу, що використовуються у проекті. Для зручного розрахунку приведемо список усього типу обладнання, що необхідно для побудови модернізованої системи безпеки на підприємстві (табл. 3.15).

Таблиця 3.2 – Опис необхідного обладнання для охоронної мережі

№	Тип обладнання	Назва моделі	Кількість
1	Контролер охоронної мережі	Ajax Hub 2 Plus	1
2	Датчик руху	Ajax MotionProtect	5
3	Датчик відкриття дверей	Ajax DoorProtect	3
4	RFID мітка	Ajax Pass Black	20
5	Датчики розбиття скла	Ajax GlassProtect	4
6	Камера відеоспостереження	Mpx Dahua IPC-K42P IMOU Cube 4MP	4
7	Мережевий екран	Ubiquiti UniFi Security Gateway	1
8	Протипожежний сповіщувач	FireProtect Ajax	4
9	Сенсорна клавіатура	KeyPad Jeweller	3
10	Сирена сповіщення	HomeSiren Jeweller	1
11	Ретранслятор радіосигналу	Ajax ReX 2	1
12	Відеореєстратор	Dahua DHI-NVR2116-I	1

3.4.2 Підрахунок вартості системи

Користуючись розрахунками кількості асортименту обладнання у попередньому розділі, можна розрахувати вартість компонентів для побудови системи безпеки на підприємстві. Проведемо розрахунок кошторису (табл. 3.15)

Таблиця 3.15 – Розрахунок необхідного обладнання для охоронної мережі

№	Назва обладнання	Кількість	Вартість за одиницю, грн	Сума, грн
1	Ajax Hub 2 Plus	1	7499	7499
2	Ajax MotionProtect	5	1499	7495
3	Ajax DoorProtect	3	1099	3297
4	Ajax Pass Black	20	850	17000
5	Ajax GlassProtect	4	1649	6596
6	Mpx Dahua IPC-K42P IMOU Cube 4MP	4	3813	15252
7	Ubiquiti UniFi Security Gateway	1	5719	5719
8	FireProtect Ajax	4	1999	7996
9	KeyPad Jeweller	3	2299	6897
10	HomeSiren Jeweller	1	1649	1649
11	Ajax ReX 2	1	4399	4399
12	Dahua DHI-NVR2116-I	1	6560	6560
			Загальна сума, грн	90 359

Отже за розрахунками кошторису вартість усього обладнання системи безпеки та контролю доступу для даного проєкту складає 90 359 грн.

ВИСНОВОК

У даному розділі було описано об’єкти на підприємстві що потребують захисту. Для їх захисту визначено місцерозташування компонентів системи безпеки, а саме: датчиків руху, відкриття дверей, розбиття скла, IP камер відеоспостереження, протипожежних сповішувачів. Монтаж кінцевого обладнання у вигляді клавіатур та сирени оповіщення і розміщено головний контролер охоронної мережі у серверній кімнаті.

Після чого обладнання було змонтовано відносно свої визначений місцерозташувань та налаштоване відповідно до політики підприємства та потреби у захисті тих чи інших об’єктів.

Для інтеграції охоронної мережі у телекомунікаційну мережу підприємства було описано мережеві можливості центрального хабу та підключення систем відео нагляду до реєстратору.

У останній частині розділу було підраховано кошторис вартості обладнання для побудови даного проекту системи захисту та контролю доступу на підприємстві.

ЗАГАЛЬНІ ВИСНОВКИ

У ході даної кваліфікаційної роботи було створено три розділи, кожен описував свій етап роботи.

Перший розділ описував актуальність систем безпеки сучасних підприємств, вектори їх атаки та комплексні способи захисту підприємства із організацією систем безпеки у декількох сферах: фізичній, інформаційній та пожежній безпеці. Також були оглянути способи підключення відеокамер, брандмауерів та інше додаткове обладнання.

У другому розділі було описано загальну структуру підприємства із картою його офісної будівлі, окрім цього було проведено огляд стану комп'ютерної мережі підприємства із переліком обладнання що є у ньому.

Був проведений опис майбутнього проєкту системи безпеки із рядом вимог фізичної, інформаційної та пожежної безпеки, що повинні виконуватися для цього підприємства.

У останній частині розділу був проведений аналіз сучасного асортименту обладнання для побудови системи безпеки таке як: контролери для мережі, датчики руху, розбиття скла, відкриття дверей, системи відеоспостереження, мережеві екрани, протипожежний захист та інше додаткове обладнання.

Останній розділ описував впровадження охоронної системи на підприємство, а саме монтаж компонентів системи – датчики руху, відкриття дверей, розбиття скла, IP камер відеоспостереження, протипожежних сповіщувачі, тощо. Також було підраховано кошторис вартості обладнання для побудови даного проекту.

Розробка даного проекту система забезпечила надійний комплексний захист підприємства та контроль доступу на ньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Enterprise Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/enterprise-security.
2. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс] – Режим доступу до ресурсу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi.
3. Organization of fire safety at the enterprise. Fire safety equipment at the enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://peskiadmin.ru/en/organization-of-fire-safety-in-the-enterprise-fire-safety-in-the-enterprise.html.
4. Why Enterprises Need Comprehensive IT Security Coverage [Електронний ресурс] – Режим доступу до ресурсу: https://www.precisionsg.com/erp-blog/why-enterprises-need-comprehensive-it-security-coverage.
5. Enterprise System Security. / [Електронний ресурс] – Режим доступу до ресурсу: https://www.mhcautomation.com/blog/enterprise-system-security
6. Технології та можливості радіопротоколу Jeweller [Електронний ресурс] – Режим доступу до ресурсу: https://support.ajax.systems/uk/jeweller-radio-protocol/.
7. KNX Technology Overview [Електронний ресурс] – Режим доступу до ресурсу: https://radiocrafts.com/technologies/knx-technology-overview/.
8. Що таке Zigbee [Електронний ресурс] – Режим доступу до ресурсу: https://xterm.com.ua/novosti/chto-takoe-zigbee-i-pochemu-eto-vazhno-dlia-vashego-umnogo-doma.
9. Business Video Surveillance [Електронний ресурс] – Режим доступу до ресурсу: https://www.stanleysecurity.com/en-ca/solutions/business-video-surveillance.
10. Вітер С. Захист облікової інформації та кібербезпека підприємства / Вітер С.А., 2017.

11. What is Enterprise Cybersecurity? [Електронний ресурс] – Режим доступу до ресурсу: https://www.growth-hackers.net/what-is-enterprise-cybersecurity/.
12. ТОВ «Індустріальні Системи Автоматизації» [Електронний ресурс] – Режим доступу до ресурсу: https://www.isa.pl.ua/?page_id=2.
13. AJAX Systems [Електронний ресурс] – Режим доступу до ресурсу: https://ajax.systems/ua/.
14. Торгова марка ОКО [Електронний ресурс] – Режим доступу до ресурсу: https://око.укр/.
15. ATIS - advanced SECURITY technologies [Електронний ресурс] – Режим доступу до ресурсу: https://atis-security.com/.
16. Dahua Technology [Електронний ресурс] – Режим доступу до ресурсу: https://www.dahuasecurity.com/.
17. Cisco Secure Firewall [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/products/security/firewalls/index.html.
18. Ubiquiti Programs [Електронний ресурс] – Режим доступу до ресурсу: https://www.ui.com/download/unifi/default/default/unifi-network-application-7376-windows.

ДОДАТОК А

Переклад першого розділу

1 THEORETICAL FUNDAMENTALS OF SECURITY SYSTEMS FUNCTIONING AT THE ENTERPRISE

1.1 Relevance of security systems in the modern world

Security systems help deter attackers from infiltrating businesses, as well as constantly protect physical and information assets. The importance of security systems cannot be overestimated, but let's list the main reasons and features that the installed security system provides to the enterprise [1, 4]:

- Minimization of possible losses – of course, modern security systems can be quite expensive, but in return they are good value for money, as they protect the investments and assets of the enterprise, which cost much more.
- Safe working environment – the company is responsible for the health and safety of its employees. The installation of security systems contributes to the creation of a safe working environment, ensuring constant control over employees. In the event of an accident or malicious acts, an immediate response is possible to solve the problem.
- Analysis of received data – with the help of various sensors and cameras, it is possible to create analytical reports and automated systems. They represent data that can improve the use of enterprise resources or facilitate the control of any emergency situations.
- Installed security systems reduce the cost of property insurance. Because insurance companies reduce the amount of payments when a business has a security system, because it leads to a reduction in risk.\

The old methods of considering information and physical security as separate entities are no longer sufficient to protect the enterprise. However, in focusing on cyber security practices, organizations often ignore their physical security needs. Security convergence combines information and physical security strategies to protect businesses from emerging threats and vulnerabilities.

Let's consider common threats to the information and physical security of the enterprise in the modern world [4]:

- External attacks – These include malicious attempts by third parties to gain information, data or physical access. Phishing, social engineering, and hacking IoT devices are all examples of threats to enterprise security from external sources. Data centers are no longer the only primary target for hackers; peripheral devices such as corporate security cameras are increasingly becoming targets of these attacks.
- Insider attacks – quite a large number of enterprise security incidents are actually carried out by employees of the organization. Issues such as property theft, vandalism, data theft and workplace violence are serious security vulnerabilities.
- Accidental security violations by employees. Inadequate security policies, unsecured networks, and outdated security systems are just a few examples of how accidental security breaches can happen. This could be for example: theft and incorrect access credentials.

Therefore, a security system is absolutely necessary for any size of enterprise. The security system will pay off in the long term for the enterprise due to the reduction of costs in malicious, emergency or unplanned situations.

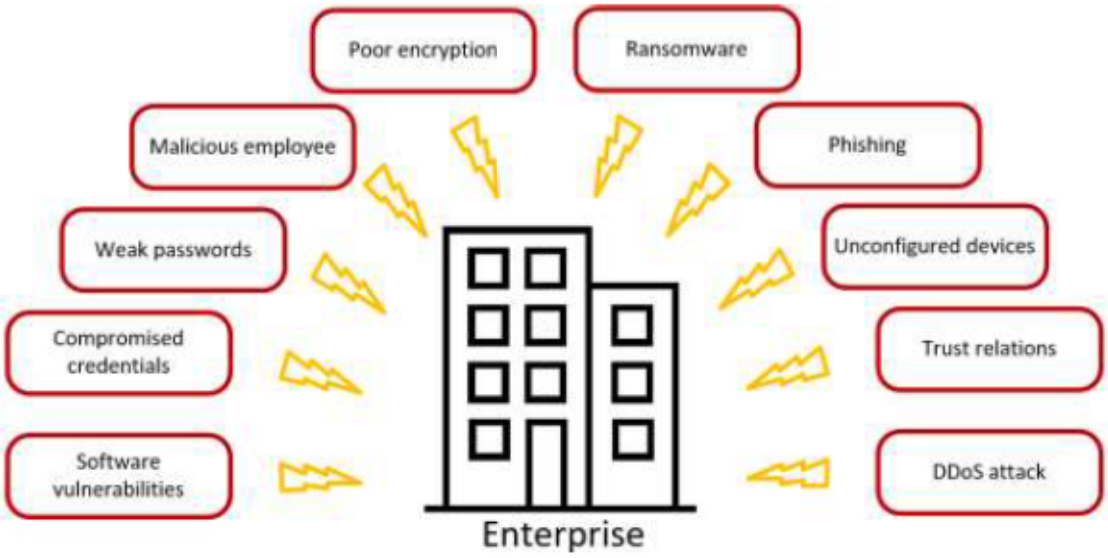


Image 1.1 – Typical attack vectors for an enterprise

1.2Modern data transmission protocols in security systems

Wireless protocols are becoming increasingly common in security systems because they allow sensors to be connected without cables, but wired protocols also have their advantages in terms of reliability. Let's list the main types of modern protocols [5,6]:

- Jeweler is a protocol developed by Ajax Systems for radio communication in security systems. Works in two directions. Supports changing the frequency of the radio channel, range up to 2 km in line of sight, protected by block encryption. Can be scaled using 5 repeaters and connect up to 200 devices. This protocol operates in the frequency range of 868.0-868.6 MHz or 868.7-869.2 MHz. Two-way communication offers advantages in the form of battery savings, when setting the standby mode on the sensors on command from the central hub. Energy efficiency is also achieved through the use of temporal distribution of channels - TDMA.
- KNX RF is the wireless version of the KNX physical layers. KNX RF can share application layers with other KNX media versions, so it is fully compatible at the application layer. The protocol operates at a frequency of 868.3 MHz using FSK modulation with a data transfer rate of 16.4 kbit/s. KNX RF allows the use of unidirectional devices (for transmission only) in addition to conventional bidirectional devices. By disabling the receiver function, the device developer can extend the battery life of the enterprise sensors.

  The typical line-of-sight range of KNX RF at 868 MHz is 150 meters. The range inside a building is highly dependent on the actual environment, building materials, etc. Under favorable circumstances, a range of up to 30 meters within a building is possible.
- Zigbee is an IEEE (Institute of Electrical and Electronics Engineers) standard for wireless home networks [8]. It is a low-power, safe technology for Smart House and security systems. Low power consumption: ZigBee allows devices to consume very little power. This makes it suitable for use with battery-powered devices such as security cameras. ZigBee has low latency, which means it can easily transmit high-speed data (such as images and videos). Strong security: ZigBee uses strong encryption and authentication algorithms that protect your data from cyber threats.

Easy installation: ZigBee devices are easy to install as they work with widely available Wi-Fi or Z-Wave gateways and home automation systems.

- KNX is a control system that was developed for seamless interaction of products from different manufacturers. The system runs on a standardized bus cable that allows different products to work together. This protocol can control all aspects of home and building management, security and door communication, audio and video, and metering. The KNX protocol uses one shielded cable pair to connect all KNX devices (switches, actuators, etc.) into a bus system. Each device in the system is assigned an individual address, allowing other devices in the system to securely route and exchange data for control (turn on lights) and feedback (room temperature).

1.3 Principles of comprehensive security and control at the enterprise

1.3.1 Provision of physical protection

Physical security measures are designed to protect buildings and protect equipment inside. They keep out unwanted people and grant access to authorized persons. While information security is also important, preventing physical security breaches is key to protecting the technology and data of the enterprise and any personnel who have access to the building. The physical security of a company and its private offices is a vital element of overall security as it prevents the loss of life and property, as well as the theft of valuable time, money and information [1,4].

There are several ways to install physical security around the enterprise:

- Make sure of the strength of the door and window frames, as this is the first vector of a physical attack on the enterprise.
- Installation of security alarms to warn of potential intruders. This will allow any suspicious activity to be recorded and appropriate measures to be taken.
- Enterprise perimeter protection – a fence with security zone violation sensors. It is also worth considering the possibility of installing high-quality security lighting.

Let's consider the main aspects of the physical security of the enterprise:

- Detection – help identify a potential security event or attacker. Sensors, alarms, and automatic notifications are all examples of physical security detection.
- Containment is a physical security measure that prevents people from leaving the space. Security components can be physical barriers such as walls, doors and windows. Access control systems and CCTV cameras also prevent unauthorized persons from trying to gain access to the building.
- Delay – There are certain security systems that are designed to slow down intruders when they try to break into a facility or building. Access control, such as requiring a key card or mobile phone credentials, is one method of delay.
- Response – reaction to when a violation or intrusion occurs. Examples of physical security responses include communication systems, building lockdowns, and calling emergency services or security responders.

Physical access control systems – allow you to regulate and manage access to enterprise doors. Installation of an access control system provides protection against uncontrolled entry points - open doors, windows, unauthorized access to sensitive areas and uncontrolled access by ordinary visitors. Below is a list of functions that a physical access control system should perform [4].

- Access restrictions – access to enterprise assets, such as servers and network equipment, to key personnel only.
- Management of access keys to entry points – doors, windows, gates.
- Integration with video surveillance systems.

1.3.2 Video surveillance systems

One of the main parts of the security system is video surveillance. Cameras are part of any good security strategy, commercial video surveillance systems give you a picture of what's going on in a building. Let's list the main characteristics of video surveillance systems used in enterprises [7]:

- Night vision or low light settings – CCTV systems can be equipped with night vision, this is especially useful for monitoring after hours or in open spaces. With its help, it is possible to get clear images even in the dark.

- Remote Pan/Tilt/Zoom Capability – Sometimes you may need the ability to zoom, tilt, or change the camera view. These types of cameras are usually more expensive than simpler dome cameras.
- Weatherproof – If the camera system is installed outdoors, you will need hardware that can withstand weather conditions.
- Built-in motion sensor – such a video surveillance system will record video only if it detects motion in the frame. This can help reduce storage costs and enterprise network requirements.
- Integration with the enterprise network - the camera can record recordings in the cloud storage or the server is located in the enterprise building. This approach makes it easy to connect access control systems, alarms, security platforms and other software tools for a more holistic approach to security.

There are a lot of cameras for video surveillance systems, but there are two main camera systems used in businesses: wired and wireless. Let's list their main differences [7]:

- Wired commercial security cameras require a cable that runs to a central hub that transmits data and video. The main advantage of a wired business video surveillance system is that there is no need to worry about a weak or poor signal. Since the connection is made using coaxial cables or PoE cables, the video surveillance recording will always be reliable as long as there is power.
- Wireless cameras send video over Ethernet or Wi-Fi. Wireless cameras can be connected directly to a power source or run on batteries. Wireless business video surveillance systems are often cheaper to install than wired ones.

According to the principle of video signal transmission, there are camera systems:

- Analog video cameras – These types of video surveillance systems use coaxial cables to transmit video and data. Setting up a commercial CCTV camera system is quite simple as each camera is connected to a power source and routed to a local video recorder (DVR). Analog video surveillance systems are a good way to provide visual monitoring. Although analog CCTV cameras are often cheaper per

unit, they can be more expensive due to the cost of cables and have limited analytics and recording functionality compared to digital video cameras.

- IP cameras (digital cameras) are network surveillance cameras that transmit images via Ethernet, and many do not require an additional power source or cable (PoE). This makes IP camera systems easier to install than analog or business video surveillance systems. In addition, they support higher quality video, some IP camera providers support video quality up to 4k with greater zoom capabilities. However, IP camera systems are often more expensive than analog video surveillance systems. With built-in data encryption and compression, as well as network security measures, IP video surveillance systems for businesses offer greater reliability and security compared to traditional systems.

Power-over-Ethernet (PoE) switches provide both power and data over a single network cable for IP camera systems. One of the advantages of using a PoE switch for commercial video surveillance is that it is easier to install, maintain, and troubleshoot. Managed PoE switches provide a wider range of settings, which is useful for controlling the output power for each camera. Since PoE switches have an IP address, it is possible to log into the system remotely via a web browser to check system status, configure parameters, and optimize the operation of video surveillance systems.

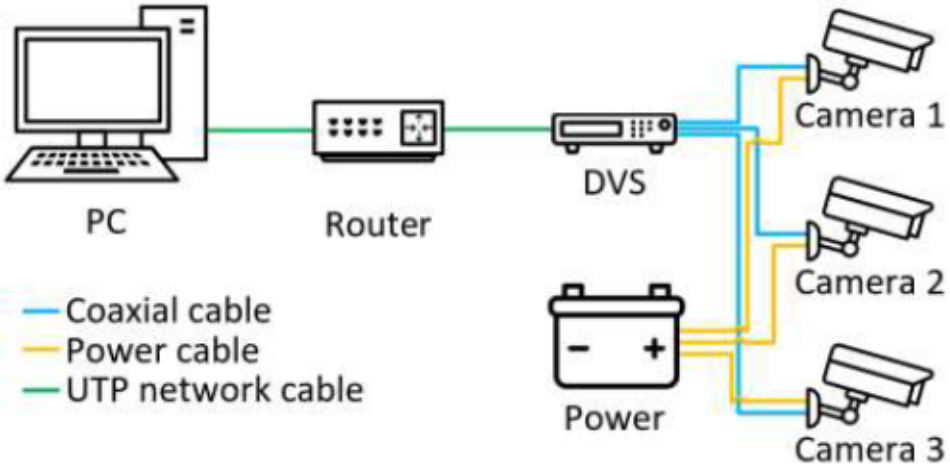


Image 1.2 Analog camera connection diagram

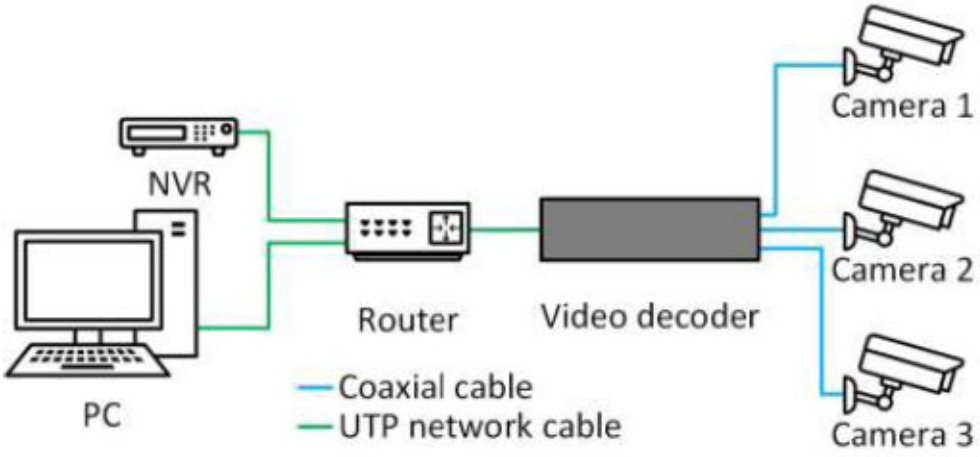


Image 1.3 Digital IP camera connection diagram

1.3.3 Information security of the enterprise

The company's information security system (cyber security) is the practice of protecting the company's data and resources from cyber threats. Cybersecurity must ensure local data protection and data transmission between networks, devices and end users. Enterprise cybersecurity not only deals with common security issues such as denial-of-service (DoS) attacks, social engineering, and software vulnerabilities. But beyond that, you also need to consider how data is transferred between devices and networks within the organization as a whole to ensure a comprehensive security system [8, 9].

In order to successfully create an information security system at the enterprise, three basic principles must be followed [8]:

- Availability of data. Accessibility ensures efficient and reliable access to information for authorized persons. The network environment must be predictable in order to access information and data when needed. If there is a failure, the system must be able to recover and such recovery must also be ensured in such a way that it does not affect other data negatively.
- Confidentiality of information. That is, the implementation of access control to ensure a reliable level of security for enterprise data, assets and information at various stages of business operations to prevent unwanted or unauthorized access. Confidentiality must be ensured when storing information, as well as forwarding it through other organizations, regardless of its format.

- Data integrity. Company information must be internally and externally consistent. Integrity also guarantees the prevention of information distortion.

Let's describe the types of modern information threats that may exist in the enterprise [9]:

- SQL injection – this attack targets the enterprise site and database directly. If successful, an attacker can inject a piece of SQL code that, when executed, provides access to sensitive information or even grants edit privileges to the database.
- A DDoS (Distributed Denial of Service) attack is a direct attack on an enterprise network. The target of the attack is the server, which would put it in a non-working mode for various purposes. Attackers can also use this type of attack to hide other attack vectors that are more difficult to identify.
- Data leakage is a security breach. Confidential data is stolen or copied by unauthorized persons. Insecure passwords can often be the root cause of this, but it can also be caused by: phishing emails, malicious security on removable media or social engineering.

Information threats and data breaches can be prevented and mitigated through good enterprise information security practices, such as security scope design and definition, enterprise architecture study, and the use of traditional cybersecurity practices. We will describe the methods that can protect the company from information threats [9]:

- Multi-factor authentication for enterprise employees is a powerful feature to prevent unauthorized users from accessing sensitive data. For the most secure user login, you should use elements such as biometrics, SMS/text messages, emails.
- Continuous employee training to reduce human error during downloads or social engineering threats. One of the most important aspects of enterprise security is educating employees on how to stay safe online. Protecting the corporate network goes beyond the IT team—everyone needs to be aware of security policies, compliance regulations, and potential vulnerabilities such as phishing or social engineering schemes.

- The policy of reliable passwords is the use of the following practices: long passwords (from 15 characters), a combination of different characters, without using dictionary words, changing passwords regularly (once a month), using a password manager.
- Detailed review of all potential threats, including employee personal devices, use of temporary passwords, two-factor or multi-factor authentication.
- Backing up data is one of the best ways to protect personal and business data from ransomware attacks. You can ensure the protection of enterprise data by implementing permanent backup. It is possible to use cloud storage or a copy of your data on the company's server. If the system was hacked, data recovery is possible.

Separately, such an important link in ensuring the information security of the enterprise as a network screen (Firewall) should be considered. A network screen or firewall is a piece of firmware or software that manages and enforces rules about what types of data packets can pass through an enterprise network, as well as other aspects of network security. A network firewall is the most important building block of any enterprise's cybersecurity infrastructure.

There are two main options for protecting your network with network screens. These two options have their pros and cons.

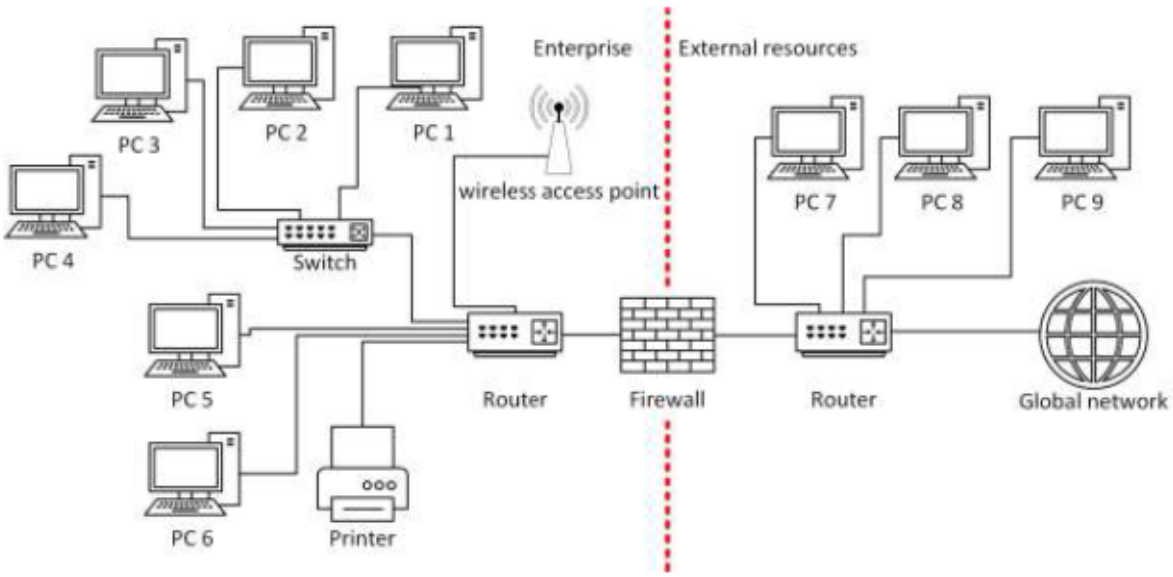


Image 1.4 – An example of using a network screen at an enterprise

A network firewall is the primary type of firewall. A network firewall is located directly between two or more networks. This is usually the dividing line between a local area network (LAN) and a wide area network (WAN), but the contours of a network firewall can be defined as the enterprise sees fit. A network firewall can typically be part of dedicated or general-purpose network traffic monitoring equipment, but fully virtual network solutions also exist.

Firewalls can prevent the following enterprise security threats [9]:

- Remote login of unauthorized users.
- Programs that install features that allow hidden access.
- Denial of Service (DDoS) when an enterprise network is overwhelmed with generated network traffic, causing computers on the network to slow down or crash.
- Network-spread viruses and worms, small programs that can spread over a network to other unprotected computers.

Web application firewalls (WAFs) are a type of application that work directly with web applications. A web application firewall sits in front of web applications and monitors both inbound and outbound web traffic. Web application firewalls because they analyze data more thoroughly than network firewalls. Let's describe their features:

- Simple configuration – web application settings and functionality are compatible with web application firewalls and can be updated on the fly to meet the requirements of new digital threats or equipment that has been added to the corporate network.
- Compatibility – A web application-based firewall is built for any web application. This means that business conducted online through a browser can be protected regardless of the application. Complex operations that cannot afford to isolate their networks will appreciate the flexibility provided by web application firewalls.

1.3.4 Fire Security

A fire alarm system in a business is designed to notify of an emergency so that people can take action to protect themselves, staff and the business as a whole.

At the heart of a fire safety system are detection devices, from sophisticated intelligent smoke detectors to simple manually operated units. There is a wide range of different types, let's describe them [3]:

- Thermal detectors – can operate based on a fixed temperature detection where it triggers an alarm if the temperature exceeds a preset value, or they can operate on a rate of temperature change.
- Smoke detectors – there are three main types of smoke detectors, according to the type of smoke detection: ionization, light scattering, light dimming.
- Carbon monoxide detectors – Carbon monoxide detectors, also known as CO fire detectors, are electronic detectors used to indicate a fire by detecting the level of carbon monoxide in the air.
- Multi-sensor detectors – such detectors combine input data from optical and thermal sensors and process them using a complex algorithm built into the detector circuit. When polling the control panel, the detector returns a value based on the combined feedback from the optical and thermal sensors. They are designed to be sensitive to a wide range of fires.
- Manual call points – A manual call point or broken glass call point is a device that allows staff to raise the alarm by breaking a fragile element on the panel; it is alarming.

Let's consider smoke detectors in detail:

- An ionizing smoke detector usually contains two chambers. The first is used as a reference to compensate for changes in ambient temperature, humidity or pressure. The second chamber contains a radioactive source, usually an alpha particle, which ionizes the air passing through the chamber, where a current flows between two electrodes. When smoke enters the chamber, the current flow is reduced. This drop in current flow is used to trigger an alarm.

- Light-scattering smoke detector - works according to the Tyndall effect; the photocell and the light source are separated from each other by a darkened chamber so that the light source does not fall on the photocell. The passage of smoke into the chamber causes the light from the source to scatter and fall on the photocell. The photocell output is used to initiate an alarm.
- In a light-obscuring smoke detector, the smoke blocks the light beam between the light source and the photocell. A photocell measures the amount of light it receives. A change in photocell power is used to trigger an alarm.

Fire alarm systems can be divided into four main types, let's list them [3].

- Traditional fire alarm systems - in this type of fire alarm system, physical cables are used to connect several detectors and detectors, the signals from which are sent back to the main control unit.
- Addressable Fire Alarm Systems - The detection principle of an addressable system is the same as a conventional system except that each detector is assigned a set address and the control panel can then determine exactly which detector or detectors initiated the alarm.
- Intelligent fire alarm systems - in such a system, each detector actually contains its own microcontroller that assesses the environment and reports to the control panel. In essence, intelligent systems are much more complex and involve many more facilities than conventional or addressable systems. Their main purpose is to help prevent false alarms.
- Wireless Fire Alarm Systems – The last type of system we will look at is the wireless fire alarm system. It is an effective alternative to traditional wired fire alarm systems for all applications.

Technical functions of the fire alarm system [3]

- detect a fire in the early stages of its development;
- transmit alarms to fire alarm devices;
- generate control signals for fire protection systems and other engineering equipment involved in fire and rescue operations;

- to signal a detected malfunction that may negatively affect the normal operation of the system.

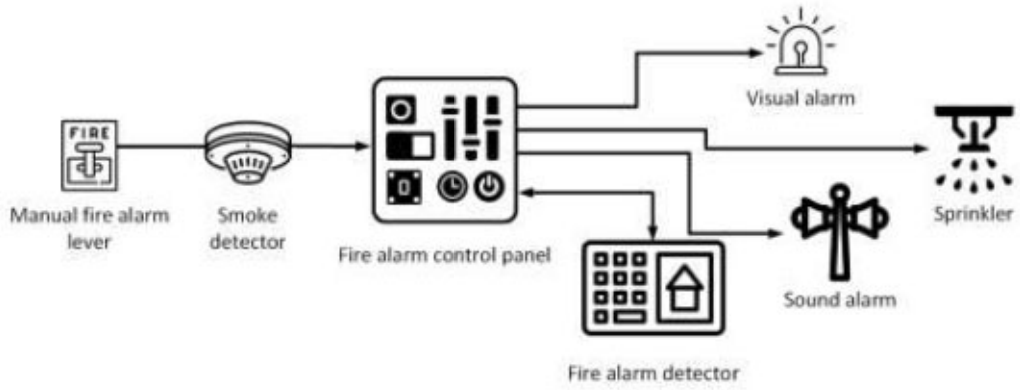


Figure 1.5 – Example of fire alarm connection at the enterprise

CONCLUSION

In the course of the first chapter, the relevance of security systems of modern enterprises was reviewed. Typical threats to them, internal and external attacks on the physical and informational security of the enterprise are considered. An overview of popular data transmission protocols in security systems, their wired and wireless versions, range and energy efficiency was also reviewed.

In the future, modern methods and principles of complex protection of the enterprise with the organization of security systems in several areas were analyzed: physical, information and fire safety. Video surveillance was also considered separately, its importance for comprehensive protection was assessed, two types of cameras - analog and IP - were considered. Connection diagrams and their features are given for each type of camera. In the course of considering the construction of information protection, attention was also paid to network firewalls, their types and options for protecting the corporate network.

ДОДАТОК Б

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами VIII Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:
ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

04 листопада 2022 року

Полтава 2022

УДК 004.89 + 681.51

Збірник наукових праць за матеріалами VIII Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика», 4 листопада, 2022 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка».

Редколегія: О.В. Шефер (головний редактор) та ін. – Полтава: НУ «Полтавська політехніка імені Юрія Кондратюка», 2022. – 100 с.

У збірнику представлені результати наукових досліджень та розробок в області сучасних електромеханічних систем та автоматизації, електричних машини і апаратів, моделювання та методів оптимізації, енергозбереження в електромеханічних системах, управління складними технічними системами, проблем аварійності та діагностики в електромеханічних системах та електричних машинах, інформаційно-комунікаційних технологіях та засобах управління. Призначений для наукових й інженерно-технічних працівників, аспірантів і магістрів.

Матеріали відтворено з авторських оригіналів та рекомендовано до друку VII Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика». Редакція не обов'язково поділяє думку автора і не відповідає за фактичні помилки, яких він припустився.

Відповідальний за випуск - д.т.н., професор О.В. Шефер.

Редакційна колегія:

О.В. Шефер – головний редактор, доктор технічних наук, професор, завідувач кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»;

Н.В. Єрмілова – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»;

С.Г. Кислиця – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка»

Б.Р. Боряк – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій Національного університету «Полтавська політехніка імені Юрія Кондратюка».

УДК 621.39

***О.В. Шефер**, д.т.н., професор,*
***Є.М. Плутцов**, магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

МОДЕРНІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ТА КОНТРОЛЮ ДОСТУПУ З ІНТЕГРАЦІЄЮ У ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ ТОВ «ІНДУСТРІАЛЬНІ СИСТЕМИ АВТОМАТИЗАЦІЇ»

Організація безпеки підприємства — це цілісна та багатогранна концепція, спрямована на виявлення, запобігання бізнес-ризиків. До них належать зовнішні загрози, помилкові порушення правил співробітниками та ризики інших сторін. Дані клієнтів та компанії є вразливими, і їх захист є головним пріоритетом будь-якого підприємства [1].

Система інформаційної безпеки підприємства (кібербезпека) – це практика захисту даних і ресурсів компанії від кіберзагроз. Кібербезпека повинна забезпечувати локальний захист даних та передачу даних між мережами, пристроями та кінцевими користувачами. Кібербезпека підприємства не тільки має справу з поширеними проблемами безпеки, такими як атаки відмови в обслуговуванні (DoS), соціальна інженерія та вразливість програмного забезпечення. Але окрім цього також потрібно враховувати, як дані передаються між пристроями та мережами всередині організації в цілому, для забезпечення комплексної системи безпеки [2].

Наявну мережу підприємства являє собою топологію «зірка» усі вузли підключаються до мережевого маршрутизатору, він у свою чергу надає доступ у глобальну. Комп'ютерну мережу можна поділити на два сегменти:

– 100 Мбіт/с, для підключення більшості обладнання та звичайних користувачів.

– 1 Гбіт/с, для підключення серверів та специфічного обладанння, що потребує високої швидкості.

У складі мережі підприємства є два обладнання, що здатні до створення точки бездротового доступу це:

– Маршрутизатор RB951G-2HnD має 2.4 ГГц діапазон

– Маршрутизатор WF2780 – працює у двох діапазонах у 2.4та 5ГГц.

Такий підхід надає можливості підключати як застаріле обладнання так і сучасне. Все мереже обладнання підключене через комунікаційному обладнання, а саме на комутаторах DES-1024D та DGS-1008D та маршрутизаторі RB951G-2HnD.

Загалом мережа підприємства має 18 персональних комп'ютерів, 3 мережевих принтери, сервер, маршрутизатор та одне мережеве сховище (NAS).

На підприємстві побудовано систему безпеки, що включає в себе: охоронну сигналізацію, система керування доступом, системи відеоспостереження та пожежну сигналізації.

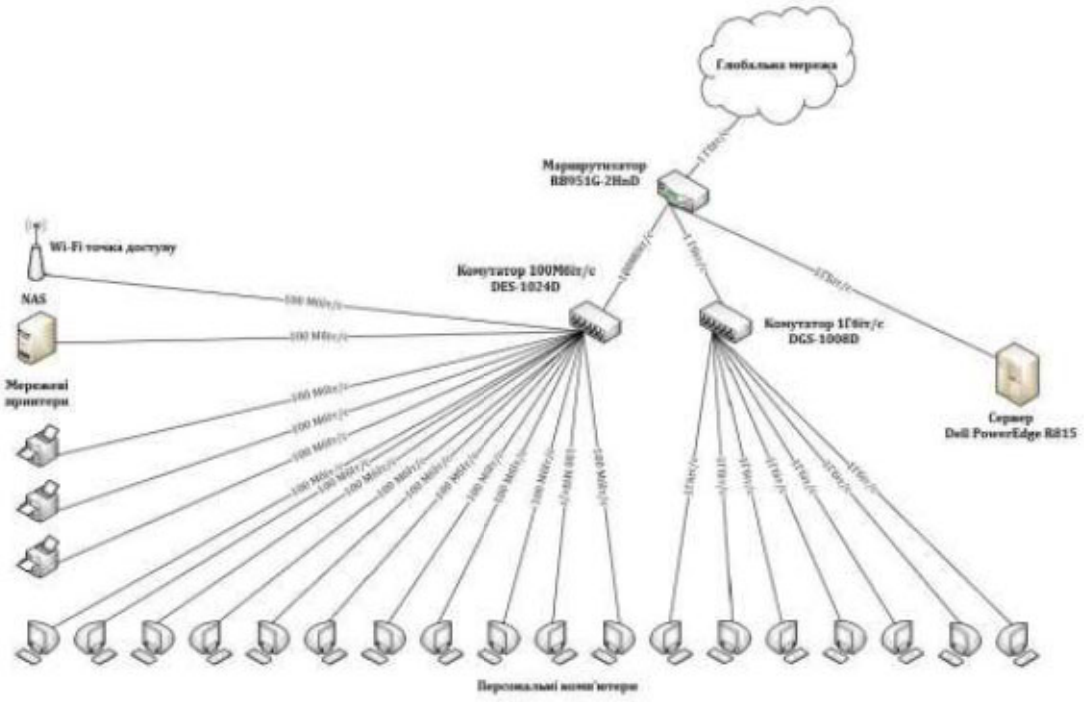


Рис. 1. Топологія мережі підприємства

ЛІТЕРАТУРА:

1. Enterprise Security [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/enterprise-security.

2. Enterprise cybersecurity / E. Scott, G. Stanley, C. Williams., 2015.

MODERNIZATION OF THE SECURITY SYSTEM OF ACCESS CONTROL WITH INTEGRATION INTO THE TELECOMMUNICATION NETWORK OF INDUSTRIAL AUTOMATION SYSTEMS LLC

***O. Shefer**, ScD, Professor,*
***Y. Pluttsov**, Master's Student*
National University «Yuri Kondratyuk Poltava Polytechnic»

УДК 004.4

***О.І. Безверхий**, д.ф.-м.н., професор,*
***В.А. Дворук**, магістрант,*
***Р.Т. Азізов**, аспірант*
Національний транспортний університет

РОЗРОБКА ТА ВСТАНОВЛЕННЯ НА ХОСТИНГ ІГРОВОГО СЕРВЕРУ ЗА ДОПОМОГОЮ JAVA ТА ORACLE CLOUD

Проаналізувавши впровадження інформаційних технологій сучасного рівня в Україні, виявлено факт недостатнього розвитку ігрових серверів в цілому, особливо дефіцит різноманітності ігрових серверів з унікальним контентом. Для

ДОДАТОК В

Демонстраційний матеріал

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра автоматики, електроніки та телекомунікацій

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРАНТА

НА ТЕМУ **МОДЕРНІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ТА КОНТРОЛЮ ДОСТУПУ З ІНТЕГРАЦІЄЮ У ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ ТОВ «ІНДУСТРІАЛЬНІ СИСТЕМИ АВТОМАТИЗАЦІЇ»**

Виконав: студент групи 601-ТТ Плутцов Є.М.

Керівник кваліфікаційної роботи: Шефер О.В.

Полтава 2022

ТЕМА: МОДЕРНІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ТА КОНТРОЛЮ ДОСТУПУ З ІНТЕГРАЦІЄЮ У ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ ТОВ «ІНДУСТРІАЛЬНІ СИСТЕМИ АВТОМАТИЗАЦІЇ»

Мета: створення проекту модернізації системи безпеки та системи контролю доступу на підприємстві.

Об'єкт дослідження: проект модернізації системи безпеки та системи доступу.

Предмет дослідження: принципи комплексного забезпечення безпеки на підприємстві, протоколи передачі даних у системах безпеки.

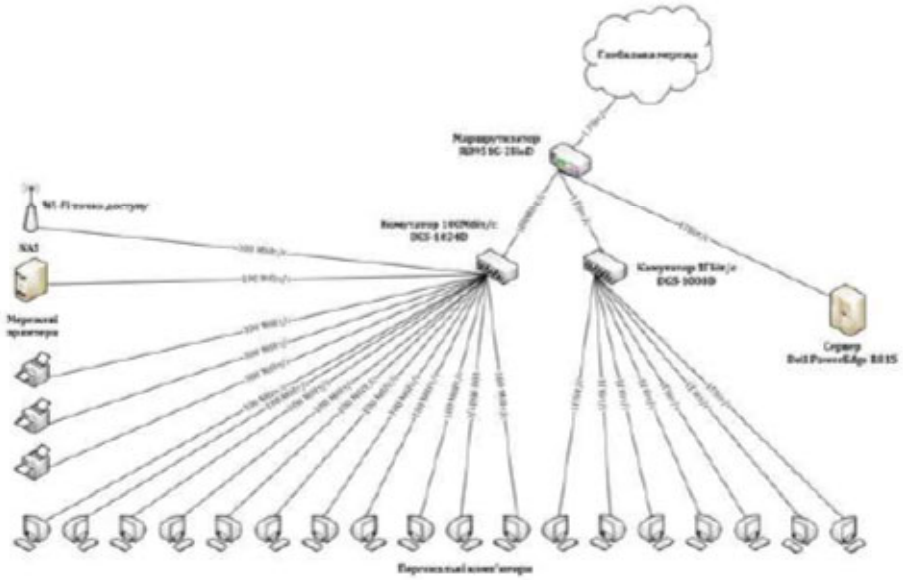
Задачі даної кваліфікаційної роботи:

- Аналіз сучасних системи безпеки на підприємстві.
- Огляд сучасних протоколів передачі даних у системах безпеки.
- Аналіз та вибір засобів та обладнання для побудови системи безпеки на підприємстві.
- Визначення розташування компонентів системи безпеки.
- Розрахунок вартості проекту системи безпеки.

КОМПЛЕКСНА БЕЗПЕКА ПІДПРИЄМСТВА

Система безпеки підприємства складається із:

- Інформаційної безпеки – захист цифрових активів та інформації.
- Фізичної системи безпеки – захист від фізичного впливу.
- Контроль доступу – розмежування доступу до приміщень/обладнання.
- Протипожежна безпека – для виявлення факту пожежі на підприємстві.

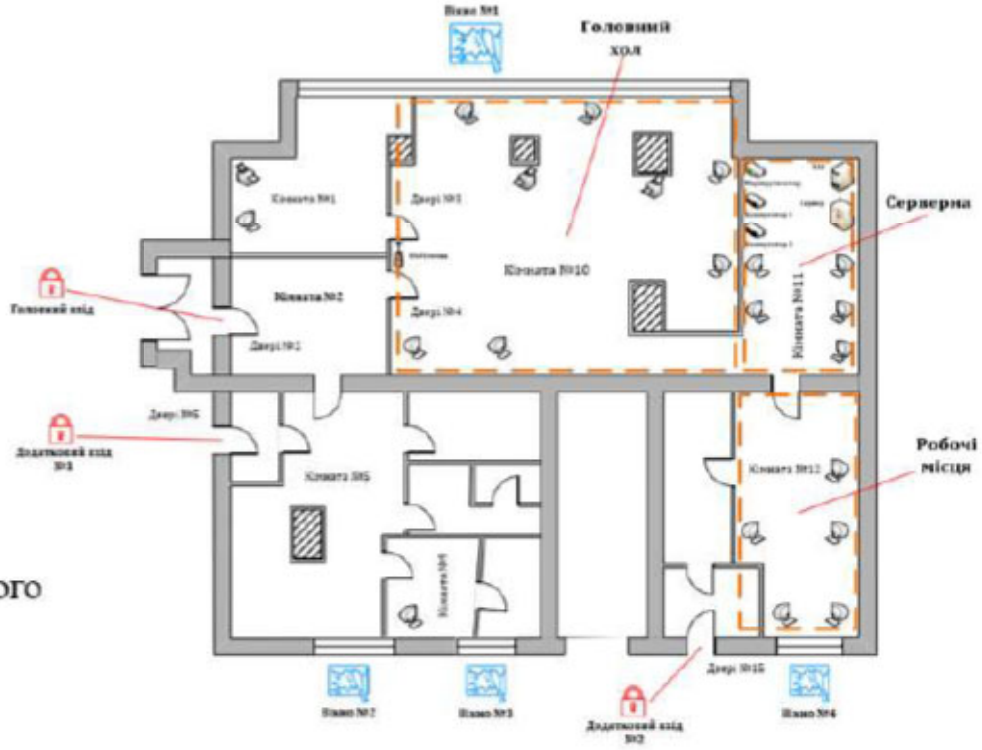


Локальна мережа та обладнання підприємства

ВИЗНАЧЕННЯ ОБ'ЄКТІВ ОХОРОНИ

Кімнати із обладнанням, що потребують підсиленого захисту:

- Головний хол.
- Серверна кімната.
- Робочі місця у кімнаті №12.



Умовні позначення

- Двері, що потребують контролю.
- Вікна, що потребують контролю.
- Кімнати, що потребують підвищеного захисту.

ОБЛАДНАННЯ ДЛЯ СИСТЕМИ БЕЗПЕКИ

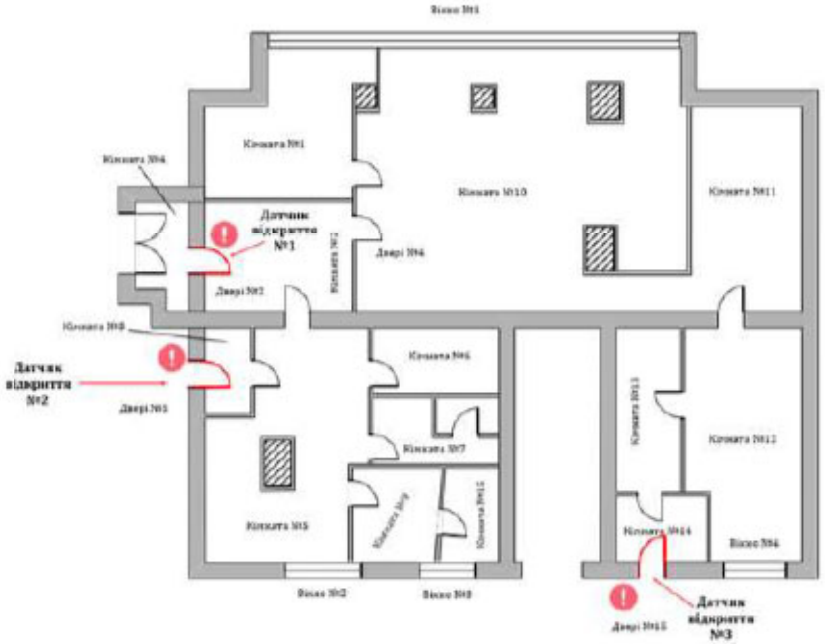
Сповіщувачі:
- Руху – Ajax MotionProtect.
- Відкриття дверей – Ajax DoorProtect.
- Розбиття скла – Ajax GlassProtect.
- Протипожежний сповіщувач – FireProtect Ajax.

Обладнання відеоспостереження:
- Відеореєстратор – Dahua DHI-NVR2116-I.
- Камера – Mpx Dahua IPC-K42P IMOU Cube 4MP.

Інше обладнання:
- Контролер безпеки – Ajax Hub 2 Plus.
- Мережевий екран – Ubiquiti UniFi Security Gateway.
- RFID мітки – Ajax Pass Black.
- Сирена сповіщення – HomeSiren Jeweller.
- Ретранслятор радіосигналу – Ajax ReX 2.
- Сенсорна клавіатура – KeyPad Jeweller.

ЗОНИ КОНТРОЛЮ ДОСТУПУ НА ПІДПРИЄМСТВІ

Зони контролю датчиків присутності



Місцерозташування датчиків контролю дверей

ІНТЕГРАЦІЯ КОНТРОЛЕРУ СИСТЕМИ БЕЗПЕКИ

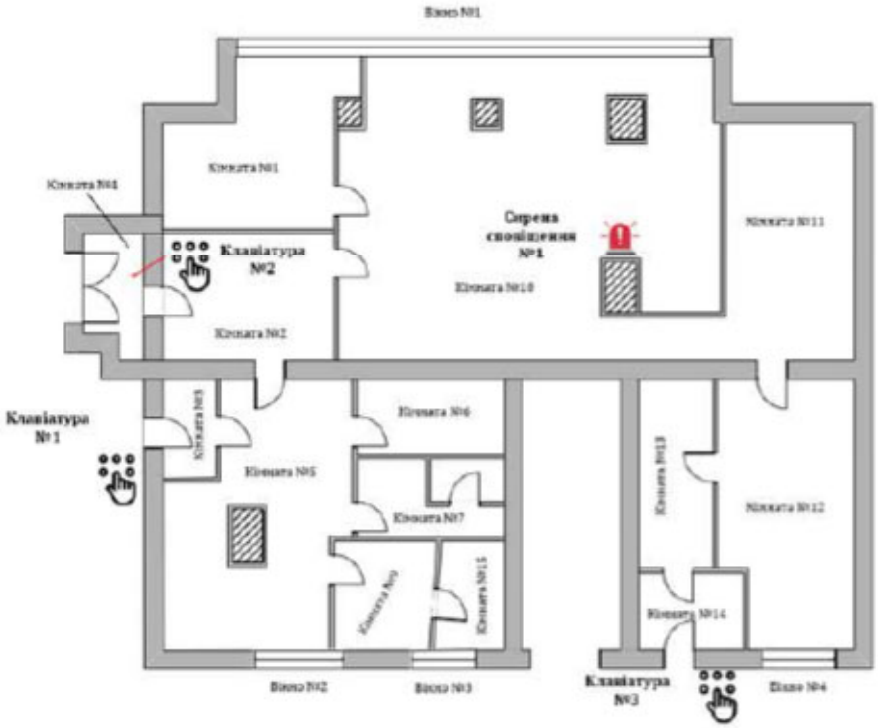
Місцерозташування контролеру

Взаємодія контролеру охоронної мережі із іншими компонентами системи безпеки

ТОЧКИ МОНТАЖУ КІНЦЕВОГО ОБЛАДНАННЯ

Характеристики кінцевого обладнання:

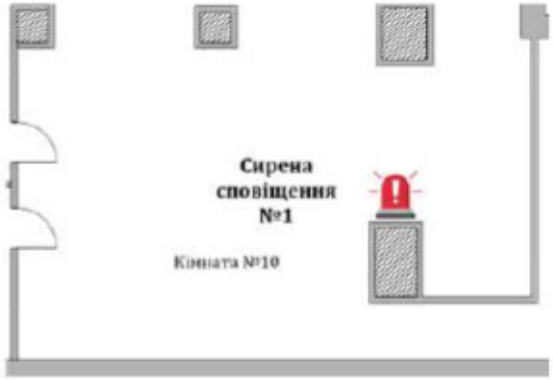
- Звукова сирена сповіщення 81-105 дБ.
- Сенсорна клавіатура введення.
- Підтримка RFID смарт-карт.
- Макс. кількість персональних кодів доступу до 99.



Монтажні місця кінцевого обладнання

МІСЦЕРОЗТАШУВАННЯ ОПОВІЩЕННЯ ТА ПРОТИПОЖЕНОЇ БЕЗПЕКИ

Розташування протипожежних сповіщувачів



Розташування сирени оповіщення

ЗОНИ КОНТРОЛЮ ВІДЕОСПОСТЕРЕЖЕННЯ

Характеристика системи відеоспостереження:

- **Тип** – цифрова IP камера.
- **Модель** – Dahua IPC-K42P.
- **Кодек** – H.265.
- **Роздільна здатність** – 2560 x 1440.
- **Кількість камер** – 4.
- **ІЧ підсвітка** – Є.
- **Макс. відео-архів** – 6 ТБ.

ВИСНОВКИ

У ході роботи були виконані поставлені завдання, а саме:

- Проаналізовано будову та структуру системи безпеки на сучасних підприємствах.
- Розглянуто протоколи, що використовуються для створення систем безпеки.
- У ході аналізу асортименту обладнання було обрано апаратні засоби та інше обладнання для системи безпеки.
- Відповідно проекту було визначено розташування обладнання та побудовано систему безпеки та контролю доступу на підприємстві.
- Розраховано кошторис загальної вартості обладнання для проекту системи безпеки.