

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: “Побудова автоматизованої системи охорони
стаціонарних видалених об’єктів підвищеної захищеності”**

на здобуття освітнього ступеня бакалавра

зі спеціальності 123 Комп’ютерна інженерія

(код, найменування спеціальності)

освітньо-професійної програми Комп’ютерні системи та мережі

(назва)

Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на
відповідне джерело

(підпис)

Олексій Овдєй
Ім’я, ПРІЗВИЩЕ здобувача

Виконав здобувач вищої освіти гр. КІД - 42

Олексій Овдєй
Ім’я, ПРІЗВИЩЕ

Керівник
науковий ступінь, ,
вчене звання

к.т.н., доцент Вячеслав Черевик
Ім’я, ПРІЗВИЩЕ

Рецензент:
науковий ступінь,
вчене звання

Ім’я, ПРІЗВИЩЕ

Київ 2024

ЗМІСТ

Вступ

1. Загальні відомості про охоронні системи

1.1 Основні принципи та завдання охоронних систем

1.2 Існуючі системи охорони

1.3 Основні компоненти охоронних систем

1.3.1 Прилад приймально-контрольний

1.3.2 Інтерфейси для керування охоронних систем

1.3.3 Датчики руху

1.3.4 Датчики розбиття скла

1.3.5 Комбіновані датчики

1.3.6 Магнітно-контактні датчики

1.3.7 Відеоспостереження

1.3.8 Системи контролю доступу

1.4 Сучасні технології в охоронних системах

1.5 Основні принципи роботи охоронних систем

2. Архітектура та технічні вимоги до охоронних систем

2.1 Архітектура охоронних систем

2.1.1 Централізована система керування

2.1.2 Інтеграція охоронних систем

2.1.3 Системи комунікацій та зв'язку

2.2 Технічні вимоги до охоронних систем

2.2.1 Надійність та стійкість

2.3 Аналіз та управління ризиками в охоронних системах

3. Побудова автоматизованої системи охорони

3.1 Огляд та аналіз об'єкту на потенційно небезпечні та вразливі місця

3.1.1 Аналіз можливих ситуацій на об'єкті

3.2 Вибір охоронної сигналізації

3.2.1 Розміщення охоронних приладів на об'єкті

3.3 Вибір обладнання для відеонагляду

3.3.1 Розміщення відеонагляду на об'єкті

3.4 Вибір системи контролю доступ (СКД)

4. Впровадження технологій безпеки на об'єкті або охорона праці

4.1 Визначення потенційно небезпечних виробничих факторів на об'єктів

4.2 Засоби індивідуального захисту та перша медична допомога

4.3 Професійна підготовка та навчання працівників з питань охорони праці

4.4 Організація навчання та перевірка знань з охорони праці

4.5 Вимоги безпеки в аварійних ситуаціях

4.6 Робота з електроінструментами

Висновки

Перелік умовних позначень

Список використаних джерел

Додаток А Презентація

Додаток Б Схема об'єкта з розташуванням охоронних приладів

Додаток В Схема об'єкта з розташуванням відеонагляду

Додаток Г об'єкта з розташуванням системи контролю доступу

Вступ

З кожним роком вимоги до безпеки стають все більш складними і високотехнологічними, особливо на віддалених об'єктах, які відіграють важливу роль у сучасному житті. Розвиток галузі у сучасному світі, де технологічний процес знаходиться на вищому рівні, питання забезпечення безпеки стає все більш актуальним та складним. Особливо важливим є захист стаціонарних видалених об'єктів, які можуть знаходитися у віддалених та важкодоступних місцях. Побудова ефективних охорони систем для таких об'єктів стає необхідною задачею у середовищі сучасних викликів і загроз, збільшення кількості та складність загроз вимагають постійного вдосконалення та адаптації заходів безпеки.

Метою даної бакалаврської роботи є дослідження та розробка автоматизованої охоронної системи безпеки для стаціонарних віддалених об'єктів з використанням новітніх технологій у даному напрямку роботи. Проект передбачає комплексний підхід щодо максимально ефективної безпеки за допомогою систем відеонагляду для постійного моніторингу, охоронних систем для повного блокування захистом важливих об'єктів.

Принцип роботи охоронної системи дуже простий. Монтажник обстежує будівлю на наявність можливих точок проникнення і блокує їх охоронними датчиками (вікна та двері є найбільш вразливими). У приміщенні охорони встановлюється сигналізація. Якщо відчиняються двері або вікно, розбивається скло або відбувається несанкціоноване проникнення на об'єкт, спрацьовує відповідний датчик і подається сигнал на прилад приймально-контрольний який у свою чергу передає сигнал тривоги на пульт централізованого спостереження та мобільний додаток, або спрацьовує звукова сигналізація, яка сповіщає охоронців, що хтось проникнув на об'єкт. Найпоширеніші датчики, що використовуються в охоронних сигналізаціях, - це інфрачервоні датчики руху, датчики розбиття скла та геркони (магнітні контакти).

Основним завданням є розробка охоронної системи яка здатна виявляти потенційні загрози в режимі реального часу та реагувати на них, забезпечуючи реагування, а також прогностичні дії у сфері безпеки на віддалених територіях. Дослідження спрямоване на пошук інноваційних рішень для впровадження високотехнологічних та ефективних заходів захисту, необхідних для забезпечення стійкості та безпеки об'єктів у віддалених районах.

1. Загальні відомості про охоронні системи

Охоронні системи є невід'ємною частиною сучасного життя, захищаючи як, майно так і людей. Охоронні системи призначені для запобігання несанкціонованому доступу, виявлення та реагування на потенційні загрози. Ці системи включають в себе широкий спектр обладнання, програмного забезпечення, спрямованих на забезпечення безпеки та порядку на території. Охоронні системи включають такі компоненти, як відеоспостереження, контроль доступу, охоронні системи та пожежна сигналізація. Ці компоненти працюють разом, щоб забезпечити загальний захист об'єкта.

Однією з найважливіших особливостей охоронних систем є інтеграція та взаємодія між компонентами. Це дозволяє створювати комплексні рішення, які забезпечують більш ефективний і надійний захист. Багато сучасних систем безпеки також пропонують дистанційне керування та моніторинг через веб-ресурси, що робить їх більш гнучкими та зручними.

1.1 Основні принципи та завдання охоронних систем

Охоронні системи - це комплексний набір датчиків, відеокамер і тд., спрямованих на захист людей, майна та інформації від різних загроз. Охоронна система повинна бути здатна протистояти вторгненню, вандалізму та підпалу.

Існують окремі рекомендації з організації захисту об'єктів (банків та інших організацій), що працюють з грошима та цінними паперами. Однак всі вони характеризуються достатньою розмитістю. На практиці, в кожному випадку схема побудови системи захисту узгоджується з охоронним органом. Об'єкт приймається під охорону лише після огляду об'єкту на потенційно небезпечні та вразливі місця. Під час цього процесу найчастіше враховуються вже наявний досвід, а іноді - і інтуїція.

Основну роль в забезпеченні комплексної безпеки об'єкту відіграють технічні засоби охоронної сигналізації. Вибір та застосування охоронної сигналізації дозволяє забезпечити високий рівень захисту об'єкту від різних внутрішніх і зовнішніх загроз і небезпек. Проте недостатній підхід до цього процесу може знизити рівень безпеки і призвести втручання на охоронюваний об'єкт.

Вибір обладнання для об'єкту залежить від характеристик приміщень, його будівельних рішень, умов експлуатації та обслуговування, а також інших факторів, які впливають на охоронну систему. Етап проектування системи безпеки є критичним, оскільки саме на цьому етапі визначаються всі основні функції та структури системи безпеки.

Основні принципи та завдання охоронних систем включають наступні аспекти:

- захист людей і майна, основною метою системи безпеки є забезпечення безпеки співробітників на об'єкті, а також майна і критично важливих ресурсів;
- виявлення порушень та реагування, системи моніторингу та

відеоспостереження можуть забезпечити можливість виявлення та швидкого реагування на порушення правил і стандартів безпеки;

- інтеграція різних технологій охоронних систем можуть поєднувати різні технології, такі як відеоспостереження, контроль доступу, сигналізація та датчики руху, для забезпечення комплексного захисту;

- підвищення ефективності та автоматизації охоронних системи спрощують процес контролю та реагування на інциденти, забезпечуючи більш ефективне та швидке реагування;

- системи відеоспостереження та інші компоненти охоронних систем можуть забезпечити зберігання критично важливих даних;

Охоронні системи відіграють ключову роль у забезпеченні безпеки об'єктів, приватних будинків, офісів та державних установ.

Вибір обладнання для системи безпеки і засобів технічного захисту об'єкту визначається значимістю його приміщень та розміщенням цінностей в них. Приміщення будь-якого об'єкту можна умовно поділити на чотири категорії залежно від їхнього призначення:

1) *Перша категорія* включає приміщення з великою кількістю особливо цінних і важливих матеріальних цінностей, де втрата може призвести до серйозного збитку або навіть загрози здоров'ю і життю багатьох людей. Це, наприклад, сховища для цінних речей, склади зберігання боєприпасів, приміщення з наркотиками або секретною документацією

2) *Друга категорія* охоплює приміщення з цінностями, втрата яких може спричинити значний матеріальний збиток або загрозу здоров'ю працівників об'єкту. Це можуть бути спеціальні архіви, сейфові кімнати зберігання важливих документів, коштовності, та інше.

3) *Третя категорія* включає приміщення зі звичайними товарами та предметами, які використовуються щоденно. Сюди входять службові кабінети, торгові зали, склади продуктів та інше.

4) *Четверта категорія* охоплює приміщення з технічним обладнанням та іншими матеріалами для виробництва та господарства. Сюди входять підсобні приміщення, склади з технічними засобами, архіви з технічною документацією тощо.

1.2 Існуючі системи охорони

Огляд існуючих систем охорони включає в себе огляд різноманітних компонентів, які складають ці системи, таких як відеоспостереження, системи контролю доступу, датчики руху, сигналізація та інші. Кожен з цих компонентів має свою функцію у забезпеченні безпеки об'єкта. Технічний огляд дозволяє з'ясувати, які саме компоненти необхідні для конкретного об'єкту, а також як вони можуть бути інтегровані для досягнення максимальної ефективності та захисту. Крім того, огляд включає в себе аналіз сучасних технологій та трендів у галузі охоронних систем, таких як використання штучного інтелекту для аналізу відеопотоків або розширене використання хмарних рішень для збереження даних та аналітики. Більш детальний огляд та

опис охоронних систем буде розглянутий в пунктах 1.3 – 1.3.9.

1.3 Основні компоненти охоронних систем

Основні компоненти охоронних систем є ключовими елементами, які сприяють забезпеченню безпеки об'єкту. Ці компоненти можуть використовуватися окремо або в комбінації, залежно від потреб безпеки об'єкта. Їхня інтеграція дозволяє створити комплексну систему безпеки, яка ефективно захищає об'єкт від різних загроз.

1.3.1 Прилад приймально-контрольний

Прилад приймально-контрольний (ППК) або централь є ключовим компонентом охоронної систем (ОС) та охоронно-пожежної сигналізації (ОПС). Він служить для отримання сигналів охоронних сповіщувачів, живлення активних охоронних сповіщувачів, надання інформації через світлові та звукові оповіщувачі, а також надання імпульсу для запуску приладів пожежного управління. Українські стандарти для ППК визначені у Державному стандарті України EN54-2. При виборі конкретного пристрою для системи необхідно керуватися нормами, згідно з якими він сертифікований.

Розглянемо різні типи ППК за способом підключення:

1) Ajax Hub, прилад приймально-контрольний (хаб) призначений для організації охоронної сигналізації на основі бездротових датчиків та інших пристроїв, що використовують синхронну роботи каналів зв'язку: Ethernet, Wi-Fi, 2G, 3G.

Хаб Ajax є головним пристроєм у будь-якій достатньо великій системі охоронної сигналізації, наприклад, квартири або будинку, і призначений координувати роботу всіх елементів охоронної системи та має автоматичне керування процесом охорони і оповіщенням тривоги.



Рисунок 1.1 – Бездротовий прилад приймально – контрольний Ajax Hub

Таблиця 1.1 – Характеристики приладу приймально – контрольного Ajax Hub

Опис	Характеристики
Процесор	ARM
Спосіб підключення приладів	Бездротовий
Канал зв'язку	2G, 3G, Wi-Fi, Ethernet
Частота GSM мережі	850/900/1800/1900 МГц, WCDMA 900/2100 (B8/B1)
Перемикання між 2G і 3G	моментально
Робочий частотний діапазон	868-868,6 МГц
Дальність дій радіосигналу	2000 м (пряма видимість)
Макс. кількість бездротових пристроїв, що підключаються	150
Тамперний вихід	реагує на відкриття корпусу
Управління	виносна клавіатура, брелок, моб.телефон, комп'ютер
Блок живлення	Вбудований
Живлення	від мережі 110-240 В, 50 Гц
Термін роботи без підзарядки живлення	16 год.
Резервне живлення	Li-Ion акумулятор
Особливості моделі	GSM-модуль із слотами для двох SIM-карт
Діапазон робочих температур	.-10°C - +40°C

GSM-модуль Hub підтримує дві SIM-карти і забезпечує швидке перемикання між 2G і 3G. Завдяки використанню SIM-карт різних операторів, хаб забезпечується зв'язком в разі втрати однієї із мережі, тобто активується інша SIM-карта.

Підключення через Ethernet і підключення через Wi-Fi забезпечує безперебійне з'єднання з інтернетом, оскільки можна використовувати послуги різних інтернет-провайдерів. Якщо обидва провайдери вийдуть з ладу і втратять з'єднання Wi-Fi та Ethernet, Hub Plus продовжить використовувати мережу 3G для доступу до інтернету; якщо покриття 3G зникне, хаб негайно переключиться на 2G, а за необхідності - на основну мережу 3G і переключиться на другу SIM-карту з резервною 2G-мережею.

Ajax Hub Plus готовий до використання прямо з коробки - встановлення займає лише кілька хвилин завдяки кріпленню SmartBracket, а модуль Wi-Fi дозволяє встановлювати хаб там, де є сигнал Wi-Fi і немає можливості прокласти Ethernet-кабель до роутера. Вбудований блок живлення забезпечує пряме підключення до електромережі без необхідності встановлення розетки.

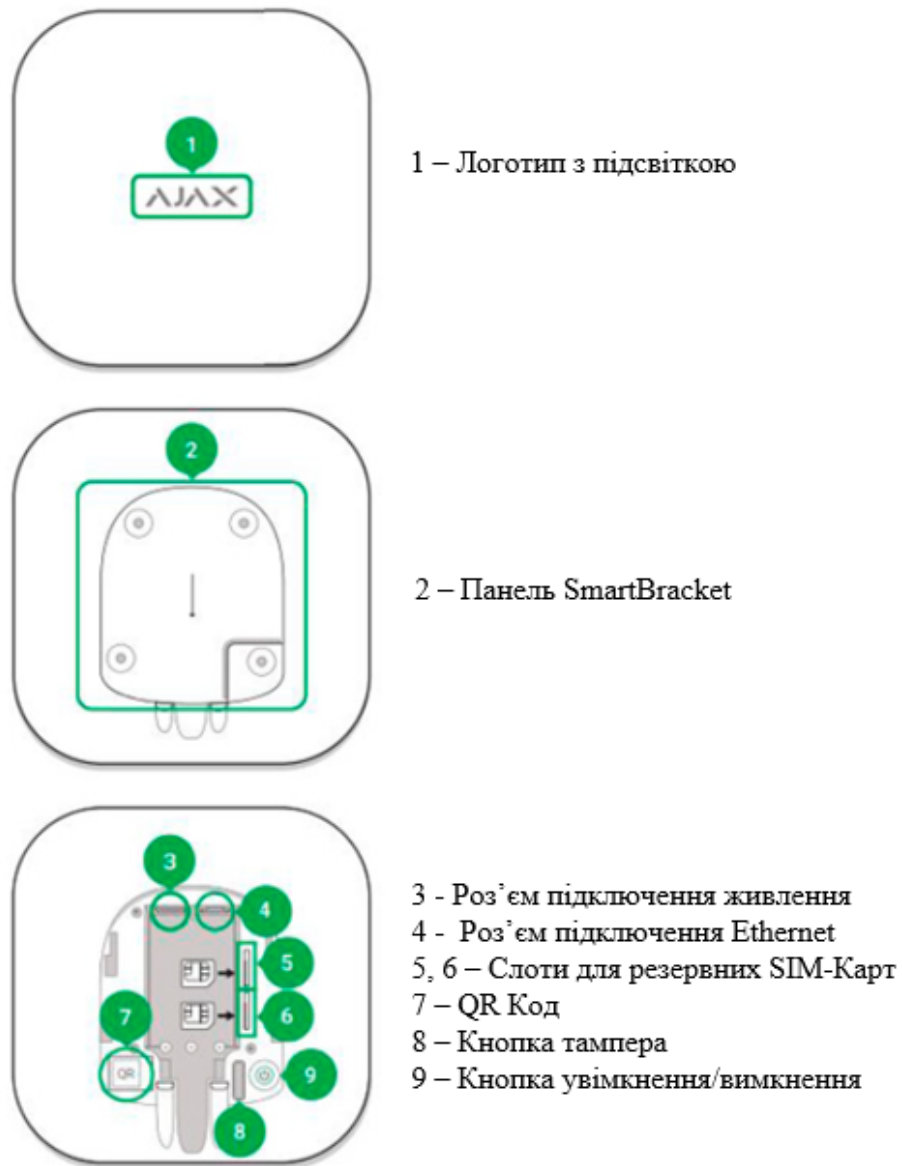


Рисунок 1.2 – Схема роз'ємів ППК Ajax Hub

Датчик підключається до ППК одним натисканням кнопки, а всі налаштування здійснюються за допомогою зручного безкоштовного додатку для телефону. Датчиком можна керувати за допомогою брелка Ajax. Датчики встановлюються в місцевості не більше ніж 2 км або на кількох поверхах будівлі. Датчики Ajax працюють без зарядки до семи років з малою кількістю спрацьовувань завдяки надійній та енергоефективній бездротовій технології (Jewelle).

Охоронна сигналізація Ajax перемикає роботу всієї системи на іншу частоту, якщо виявляє порушення сигналу. На програмному рівні хаб повністю захищений від вірусів.

Підключення до інтернету дає змогу хабу цілодобово зв'язуватися зашифрованим каналом із сервером Ajax Cloud, щоб забезпечити безпечний доступ до пристрою, збереження налаштувань і миттєве отримання оновлень.



Рисунок 1.3 – Схема монтажу ППК Ajax Hub Plus

2) Orion NOVA M – це провідний прилад приймально-контрольний, який контролює 8 зон з можливістю розширення до 32. Ці зони розділені на 16 груп і можуть контролюватися індивідуально. Системою сигналізації можна керувати дистанційно за допомогою програмного забезпечення oLoader II, мобільного додатку Control NOVA II або локально за допомогою клавіатури, брелока або зчитувача сенсорних ключів. Пристрій підтримує як автономність, так і безпеку з можливістю підключення до пульта централізованого спостереження за допомогою двонаправленого захищеного протоколу NOVA. Прилад приймально-контрольний підтримує протокол SUR-GARD (Contact ID) для взаємодії зі сторонніми пристроями моніторингу.

Вбудований пристрій зв'язку GSM (GPRS), функція контролю глушіння мережі GSM, підтримка двох SIM-карт, функція обміну SMS-повідомленнями.

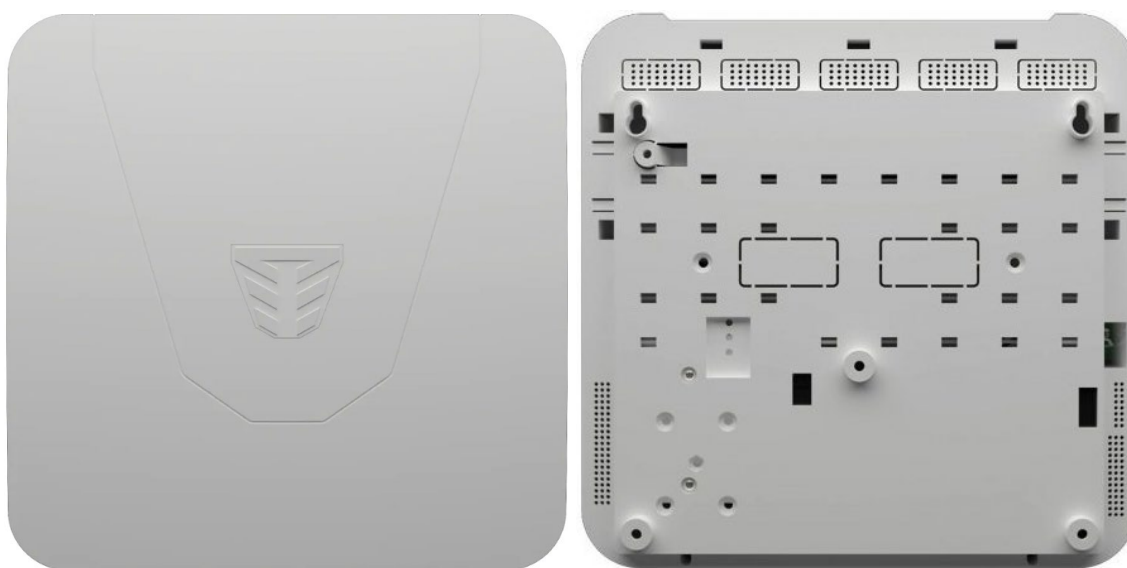


Рисунок 1.4 – Дротовий прилад приймально – контрольний Orion NOVA M

Прилад приймально – контрольний Orion NOVA M відмінно підходить для створення охоронної сигналізації з елементами «розумного будинку». ППК підходить для створення охоронних сигналізацій на об'єктах середніх розмірів. У ППК є можливість щоб організувати постановку або зняття з охорони за допомогою мобільного додатку «Control Nova ||».

При необхідності у ППК є можливість інтеграції з бездротовими датчиками (тобто потрібно підключити додатковий модуль M-WRL(A)), ППК Orion NOVA M дозволяє підключати обладнання різних фірм.

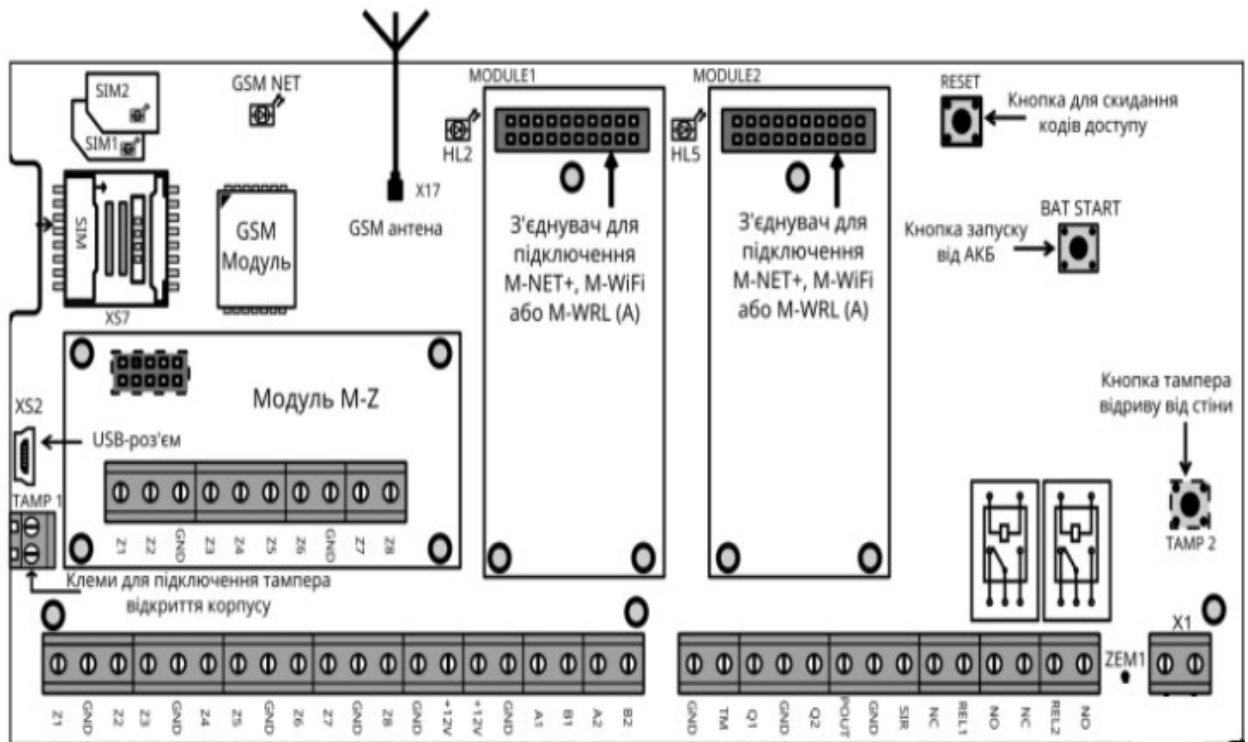


Рисунок 1.5 – Схема приладу приймально – контрольного Orion NOVA M

Плата Orion NOVA M має клеми для підключення охоронної зони, клавіатури, зчитувача ключів з сенсорною пам'яттю та сирени. Для керування зовнішніми пристроями передбачено два транзисторні виходи, до яких можна підключити зовнішні світлодіоди. У самій платі Orion NOVA M передбачено місце для встановлення акумулятора ємністю 7 Ач або 9 Ач, який діє як резервне джерело живлення у разі відсутності живлення від електромережі.

Завдяки передовим технологіям, вбудованим в цей пристрій, забезпечується висока швидкість реагування на потенційні загрози та широкий функціонал управління, що дає можливість налаштовувати систему безпеки відповідно до конкретних потреб користувача.

Крім того, прилад приймально – контрольний Orion NOVA M підтримує інтеграцію з іншими виробниками охоронних приладів, що дозволяє створювати комплексні та надійні системи захисту для різноманітних об'єктів, від житлових приміщень до промислових комплексів.

Таблиця 1.2 – Характеристики приладу приймально – контрольного Orion NOVA M

Опис	Характеристики
Спосіб підключення приладів	Дротовий
Канал зв'язку	GPRS, Wi-Fi, Ethernet
Кількість зон	8, є можливість розширити до 32
Модулі розширення	не більше 2 - M-Z та (або) M-WRL(A)
Підключення клавіатур	максимум 4
Особливості моделі	GSM-модуль із слотами для двох SIM-карт
Управління	виносна клавіатура, брелок, моб.телефон
Джерело живлення	220 В (+22 В, - 33 В) / 50 Гц
Час роботи від зарядженого АКБ	не менше 30 годин
Діапазон робочих температур	.-10°C - +40°C

1.3.2 Інтерфейси для керування охоронних систем

Клавіатура – це пристрій, який потрібно використовувати для управління та керування охоронною системою.

Клавіатура представляє собою компактний пристрій з набором кнопок та індикаторів, які дозволяють користувачу взаємодіяти з охоронною системою.

Основні функції клавіатур охоронних систем:

- Активація та деактивація, користувач може ввести код доступу за допомогою клавіатури для увімкнення або вимкнення охоронної системи.
- Відображення стану системи, індикатори на клавіатурі відображають поточний стан охоронної системи активована/деактивована.
- Сповіщення про стан охоронної системи, клавіатура може також служити для виведення аудіо-або візуальних сигналів, які повідомляють користувача про різні стани та події системи, наприклад, сповіщення про введення невірної коду або про виникнення тривоги.
- Керування охоронними приладами, тобто, датчиками, дверні замки, ворота та інше. Загалом, клавіатура охоронної сигналізації є важливим елементом системи безпеки, який дозволяє користувачам зручно та ефективно керувати та контролювати захисні функції свого об'єкту.

Отже, потрібно обрати клавіатуру для керування та програмування приладу приймально-контрольного (центрالی). Для кращої продуктивності варто обрати клавіатуру, яку можна замовити в комплекті з централлю. Тому розглянемо клавіатури середнього цінового сегменту для централей які були розглянуті у розділі 1.3.1.

1) TIRAS K-PAD OLED - це дротова сенсорна клавіатура, призначена для ідентифікації користувача та доступу до керування режимами охоронної системи. Клавіатура сенсорна призначена для програмування та управління

системою охорони Orion NOVA II (включення та виключення груп з охорони, керування автоматикою) та контролю її стану.

Сенсорні кнопки на панелі призначені для управління охоронною системою. Вони оснащені підсвіткою, яка вмикається при натисканні на кнопку. Клавіатура також має світловий індикатор, що показує стан системи (під охороною, несправність, тривога) і вбудований температурний захист від крадіжки.

Клавіатура призначена для неперервної роботи 24/7 в приміщеннях з температурою від -10°C до +40°C. Клавіатура підходить для монтажу на стіну.



Рисунок 1.6 – Сенсорна дротова клавіатура TIRAS K-PAD OLED

Таблиця 1.3 – Характеристики клавіатури K-PAD OLED

Опис	Характеристики
Тип дисплею	OLED
Тип сенсора	Ємнісний
Кількість зон	2
Транзисторний вихід	1
Підключення ППК	по системній шині RS-485
Вбудований інтерфейс	Touch Memory
Напруга живлення	9,3 - 15,2 В (входи 12V)
Струм споживання	120 мА

2) Ajax KeyPad Plus - це бездротова сенсорна панель для управління охоронною системою Ajax Systems, доповнена вбудованим зчитувачем захищених від копіювання безконтактних карт Ajax Pass і брелків Ajax Tag. Існує група сенсорних кнопок для введення коду доступу, а також окремі кнопки для активації режимів охорони, нічного режиму, вимкнення охорони, а також індикатори, що показують активність цих режимів.

Клавіатура взаємодіє з ППК Ajax через протокол Jeweller на частоті роботи 868-868.6 МГц. Максимальна відстань зв'язку складає приблизно 1700 м на відкритій місцевості без перешкод. Для забезпечення надійності системи застосовується захист від перешкод і маніпуляцій з сигналами, а також перевірка функціональності та зв'язку шляхом відправки пінгів з інтервалами від 12 секунд.



Рисунок 1.7 – Сенсорна бездротова клавіатура Ajax KeyPad Plus

Перехоплення та заміна сигналу неможлива завдяки аутентифікації та блочному шифруванню, яке ґрунтується на алгоритмі AES (систематичний блоковий шифр, який може зашифрувати/розшифрувати дані). Присутній тамперний захист, який активує сигнал тривоги при спробі саботажу, такі як відділення пристрою від монтажної поверхні або відкриття корпусу.

Сила передачі радіосигналу змінюється залежно від відстані між датчиком та централлю: чим ближче датчик до центрального вузла, тим менше енергії витрачається на передачу.

У випадку вимикання сигналізації зловмисником передбачено використання спеціального коду, який, при введенні, відправляє прихований сигнал тривоги до центральної системи та імітує відключення системи охорони. У разі спроб неправильного введення коду декілька разів поспіль, клавіатура автоматично блокується, і відправляється повідомлення про перевищення допустимої кількості спроб введення коду доступу.

Клавіатура Ajax KeyPad Plus готова до роботи з коробки - всі елементи живлення вже встановлені, а стандартні налаштування вже налаштовані. Монтаж здійснюється за декілька хвилин завдяки кріпленню SmartBracket. KeyPad Plus розміщується неподалік від входних дверей для забезпечення легкого та швидкого доступу. Підключення до системи можливе всього в один клік через мобільний додаток, просто сканувавши QR-код.



Рисунок 1.8 – Схема монтажу клавіатури Ajax KeyPad Plus

Таблиця 1.4 – Характеристики клавіатури Ajax KeyPad Plus

Опис	Характеристики
Спосіб підключення	Бездротова
Підтримка протоколу	Jeweller
Робоча частота	868.0 - 868.6 МГц
Дальність дії радіосигналу	1700 м
Зчитувач	брелок/карта
Особливості моделі	Захист від підбору паролю
	Захист від перехоплення сигналу
Діапазон робочих температур	.-10°C - +40°C

1.3.3 Датчики руху

Датчик руху - це охоронний прилад, який призначений для реагування на рух в певній зоні. Він реагує на зміни в інфрачервоному випромінюванні або ультразвукових хвилях, що відбуваються при русі людини або іншого об'єкта. Датчики руху повідомляють про перші ознаки несанкціонованого проникнення у ваш будинок або офіс. Монтується на стіні навпроти дверей або іншої потенційної точки проникнення. Датчик використовує пасивний інфрачервоний сенсор і виявляє людей за рівнем їхнього інфрачервоного випромінювання. Отримані дані обробляються цифровим способом, щоб запобігти хибним тривогам. Тому розглянемо різні типи датчиків руху такі як дроторів/бездротові.

1) Датчик руху бездротовий Ajax Motion Protect призначений для виявлення руху людини в захищеному приміщенні. Датчик має регульовану чутливість і може ігнорувати домашніх тварин вагою до 20 кг та зростом до 50 см.



Рисунок 1.9 – Бездротовий датчик руху Ajax Motion Protect

Принцип роботи датчика ґрунтується на визначенні інфрачервоного (ІЧ) випромінювання від живих істот. Кожна живе істота, у тому числі людина, є джерелом ІЧ випромінювання. Як тільки датчик виявляє таке випромінювання, він аналізує масу об'єкта, і у випадку, якщо об'єкт перевищує 50 сантиметрів та 20 кг, датчик відправляє сигнал тривоги на централь через радіоканал. Спеціальний алгоритм обробки отриманого сигналу забезпечує додаткову перевірку об'єкта щодо маси та наявності руху, щоб мінімізувати помилкові спрацювання від рухливих домашніх тварин. Таким чином, датчик спрацьовує лише при виявленні руху людини. Крім того, датчик не реагує на переміщення неживих предметів. Наприклад, в приміщенні відкриється міжкімнатні двері через протяг, датчик не спрацює.

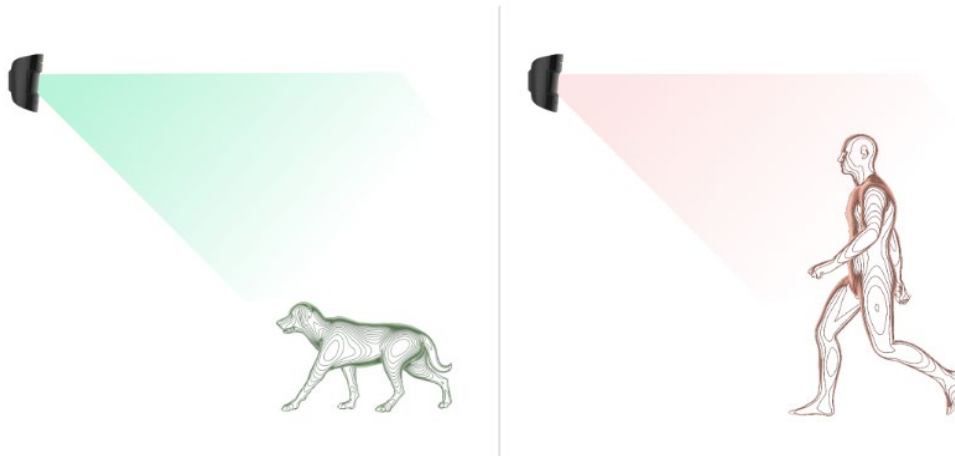


Рисунок 1.10 – Спрацювання датчика на об'єкт більше 50 см. та 20 кг.

Якщо датчики руху для приміщень встановлено нижче рекомендованої висоти, тварини будуть активні в зоні підвищеної чутливості. Навіть якщо собака підійметься на задні лапи або навіть маленький собачка поскаче на кріслі, датчик може виникнути тривогу. Також тривога буде викликана, якщо тварина має можливість дотягнутися до рівня датчика або пересуватися навколо нього.

При виборі місця встановлення датчика потрібно врахувати спрямованість лінзи, кути огляду датчика та наявність перешкод, які погіршують огляд датчика. Бажано, щоб напрямом лінзи датчика був перпендикулярний прогнозованому шляху проникнення в приміщення. Потрібно впевнитися, що меблі, домашні рослини, вази, декоративні або скляні конструкції не перекривають огляд датчика.

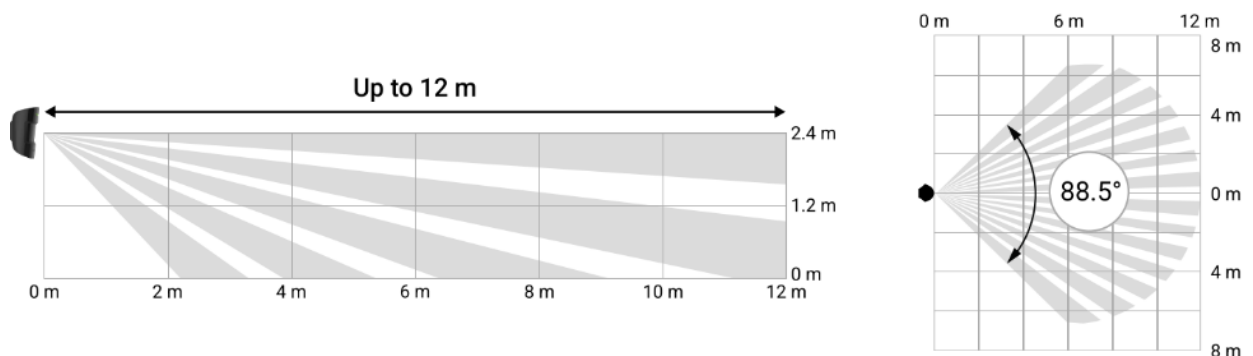


Рисунок 1.11 – Зона спрацювання датчика руху Ajax Motion Protect

За умови правильного встановлення та налаштування датчик не реагує на домашніх тварин зростом до 50 см і вагою до 20 кг, які є типовими причинами хибних тривог. Для спрощення монтажу датчик постачається з попередньо встановленою кріпильною панеллю SmartBracket. Під час встановлення не потрібно розбирати датчик, тому немає ризику пошкодити електроніку.

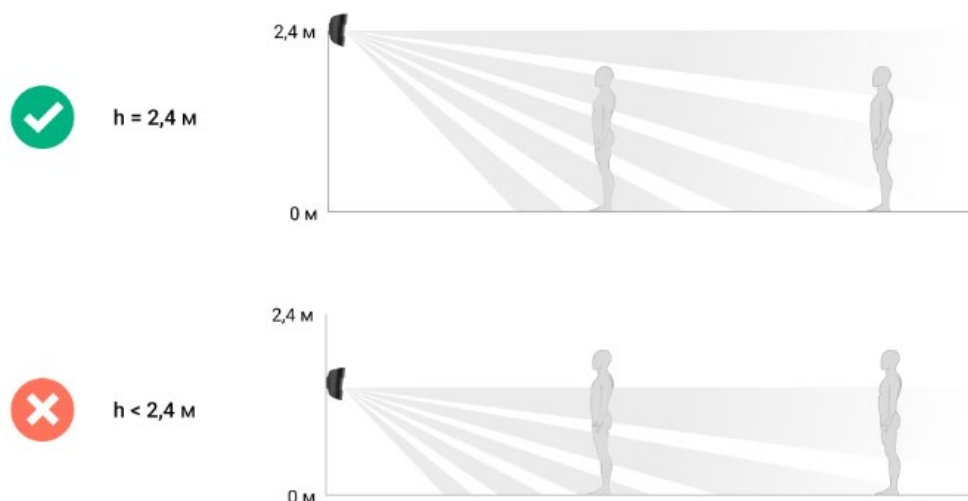


Рисунок 1.12 – Рекомендації монтажу датчика руху Ajax Motion Protect

Таблиця 1.5 – Характеристики датчика руху Ajax Motion Protect

Опис	Характеристики
Тип датчика	Бездротовий
Чутливий елемент	ІЧ сенсор
Дальність виявлення руху	до 12 м
Діапазон робочих частот	866,0 – 866,5 МГц
Живлення	1 батарея CR123A, 3В
Строк роботи від елемента живлення	до 5 років
Кут огляду датчика руху	88,5° / 80°
Шв. Виявлення руху	Від 0,3 до 2 м/с
Основні можливості	Імунітет від тварин, легке монтування

2) Дротовий датчик руху Ajax Motion Protect Fibra однаковий за своїм призначенням та спрацюванням з бездротовим датчиком Ajax Motion Protect, але відрізняється характеристиками, а саме технологією зв'язку Fibra.

Fibra – це двосторонній протокол для швидкого і безпечного зв'язку між централлю. Fibra використовує шифрування та автентифікацію для захисту від підміни пристроїв. Протокол підтримує регулярні опитування охоронних приладів для відображення їх станів у реальному часі. Дальність дротового зв'язку Fibra до 2000 м. Це надає можливість забезпечити захист об'єктів будь яких масштабів та найкращий досвід користування як для інженерів монтажу, так і кінцевих користувачів.



Рисунок 1.13 – Дротовий датчик руху Ajax Motion Protect

Сигнал Fібра визначається співвідношенням кількості недоставлених або пошкоджених пакетів даних до очікуваних за певний проміжок часу. На рівень сигналу впливають такі фактори, як кількість підключенн до однієї лінії Fібра, довжина і переріз кабелю, та точність підключення дротів до клем.



Рисунок 1.14 – Функціонал дротового датчика руху Ajax Motion Protect

1.3.4 Датчики розбиття скла

Датчик розбиття скла - це охоронний прилад, який призначений для виявлення або спрацювання у разі руйнування скла. Він реагує на характерний звук, який виникає при розбитті скла, і спрацьовує для сповіщення про можливий інцидент або викликання сигналізації безпеки. Цей тип датчика використовується для захисту вікон, дверей або скляних поверхонь в будинках, автомобілях, офісах тощо. Розглянемо різні типи датчиків розбиття скла середнього цінового сегменту.

1) Crow GBD-2 - це дротовий датчик розбиття скла. Він працює на основі схеми фазо-частотного розділення, що практично знижує кількість помилкових спрацювань до мінімуму. Не потребує монтажу на склі. Датчик може захищати кілька вікон.



Рисунок 1.15 – Дротовий датчик розбиття скла Crow GBD-2

Охоронний пристрій Crow GBD-2 працює за технологією фазо-частотного розділення. Він реагує на два послідовних сигнали - спочатку на удару по склу, а потім на дзвін розбитого скла. Така схема дозволяє уникнути помилкових спрацювань сповіщувача на звуки, близькі за частотою до дзвіну скла.

Чутливість обох частотних каналів калібрується окремо. Для цього використовується спеціальний пристрій-імітатор, що генерує звук розбитого скла. Встановлювати датчик не обов'язково на саме вікно. Він може монтуватися на стіну або стелю на висоті від 1,8 до 2,4 м. Оптимальна відстань до охоронюваного вікна - близько 4,5 м, максимальний радіус спрацювання становить 9 м., кут спрацювання 170°, джерело живлення DC 9-16 В та робоча температура становить від -20 ~ +50.

2) Glass Protect Jeweller – це датчик бездротовий розбиття скла який використовуючи електронний мікрофону для виявлення звуку удару по склу і звучання при його розбитті, встановлюється всередині приміщень, працює до 7 років від комплектної батареї. Датчик GlassProtect інтегрується у систему Ajax, використовуючи захищений протокол *Jeweller* для з'єднання з хабом. Зв'язок здійснюється на відстань до 1000 метрів.



Рисунок 1.16 – Датчик розбиття скла бездротовий GlassProtect

У GlassProtect встановлений чутливий мікрофон який налаштований для виявлення характерних звуків розбиття скла, які включають низькочастотний удар і високочастотний дзвін уламків. Цей двоетапний процес розпізнавання мінімізує можливість помилкових спрацювань.



Рисунок 1.17 – Функціонал датчика GlassProtect Jeweller

Датчик GlassProtect може виявляти розбиття на відстані до 9 метрів розбиття скла. Важливо, щоб мікрофон був розташований під кутом не більше 90° відносно вікна або вікон. Також потрібно перевірити, що жалюзі, рослини, меблі або інші предмети не перекривають мікрофон. У разі, якщо вікно закрите шторами, датчик краще встановити між ними та вікном (штори можуть приглушити звук розбиття скла, і датчик може не спрацювати).

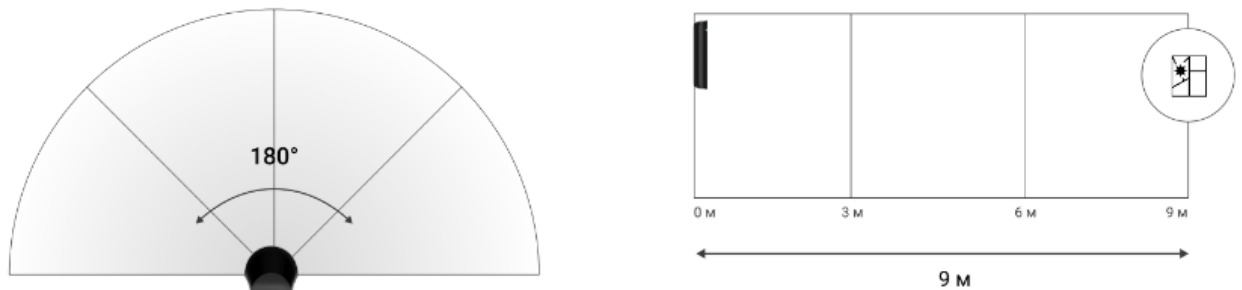


Рисунок 1.18 – Кут виявлення розбиття скла датчика GlassProtect

Ключові можливості бездротового датчику розбиття скла GlassProtect Jeweller – це фільтр хибних тривог (звуки подібні розбиттю скла будуть фільтруватись), та на одному акумуляторі до 7 років безперебійної роботи.

1.3.5 Комбіновані датчики

Комбіновані датчики - це охоронні пристрої, які об'єднують в собі кілька типів датчиків для виявлення різних видів подій на об'єкті. Ці датчики можуть включати функції, такі як виявлення руху та розбиття скла. Комбіновані датчики зазвичай забезпечують більш широкий спектр функціональності і можуть бути відмовостійким рішенням для комплексного контролю на об'єкті.

Функціональні елементи, технічні характеристики комбінованого датчика не відрізняються від датчика руху (опис датчика у пункті 1.3.3) та датчика розбиття скла (опис датчика у пункті 1.3.4), а об'єднує ці два датчика в собі.



Рисунок 1.19 – Функціонал комбінованого датчика CombiProtect

1.3.6 Магнітно-контактні датчики

Магнітно-контактний датчик – це охоронний пристрій, який реєструють стан дверей або вікон (відкрито або зачинено) і генерує сигнал у випадку будь-яких змін. Ключовою складовою частиною магнітоконтактного датчика це допомагати вчасно виявляти проникнення на об'єкт, який знаходяться під охороною. Ці датчики широко використовуються для забезпечення безпеки в будинках, офісах та інших приміщеннях.

Основний тип датчика відкриття дверей включає в себе:

– Магнітний датчик: електронний пристрій, який використовує геркон (геркон - містить електричний контакт в герметичній оболонці, який замикається внаслідок наближення магніту та розмикається віддаленням на відстань понад 1 см. Таким чином, датчик реєструє як відкриття, так і закриття дверей і вікон) для виявлення магнітних полів. Коли двері або вікно відчиняються, магніт віддаляється від геркона, що призводить до активації датчика.

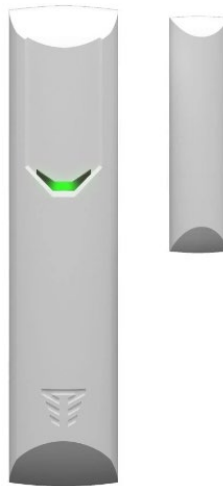


Рисунок 1.20 – Бездротовий датчик відкриття дверей Tiras X-Shift White

Бездротовий датчик відкриття Tiras X-Shift має можливість зв'язку з ППК на відстань до 3 км. Максимальна відстань між магнітом та сповіщувачем складає 15 мм на неметалевій поверхні та 4 мм на металевій поверхні. Цей бездротовий датчик використовує цифровий сенсор магнітного поля, який повідомляє про будь-які недозволені відкриття або вторгнення через вікна чи двері. Він може бути встановлений на будь-які типи поверхонь, включаючи пластик, дерево та метал.

Ключові можливості датчика відкриття дверей Tiras X-Shift White – це використання сенсора Хола (це пристрій для виміру величини магнітного поля) замість традиційного геркона має кілька переваг, включаючи можливість калібрування, захист від саботажу сильним магнітом та можливість розміщення магніта зліва або справа. Додатково, відсутність проблеми "залипання" датчика додає надійності та ефективності.

1.3.7 Відеоспостереження

Системи відеоспостереження - це інфраструктура, яка включає в себе різноманітні пристрої та програмне забезпечення для захоплення, передачі, зберігання і відтворення відеоданих з метою забезпечення безпеки та контролю за об'єктом чи територією. Ці системи використовуються у різних областях, включаючи комерційні приміщення, офіси, виробничі підприємства, громадські місця та приватні житла. Вони можуть бути складними інтегрованими системами або простими наборами пристроїв, що включають відеокамери, монітори, системи зберігання та програмне забезпечення для управління і аналізу відеоданих.

Види відеокамер можна класифікувати за декількома параметрами:

- 1) За типом монтажу, внутрішні (для приміщень) та зовнішні (для вулиці)
- 2) За типом камери:

- Аналогові (традиційні камери, які виводять відеосигнал через аналоговий кабель).

- IP-камери (камери, що підключаються до мережі через Ethernet або Wi-Fi, інтегруючи з системами відеоспостереження).

Компоненти системи відеоспостереження включають:

- 1) Відеокамери – електронні пристрої для захоплення та запису відеоматеріалів, які можуть бути розміщені в різних частинах об'єкту для забезпечення повного охоплення.

- 2) Мережеве обладнання – використовується для передачі відеоданих через мережу, таке як маршрутизатори, комутатори та інше мережеве обладнання.

- 3) Системи збереження – місце для зберігання записаних відеоматеріалів, включаючи централізовані системи збереження (наприклад, DVR з встановленим жорстким диском) або хмарні сховища.

- 4) Монітори – використовуються для перегляду відеоінформації в реальному часі або відтворення записів.

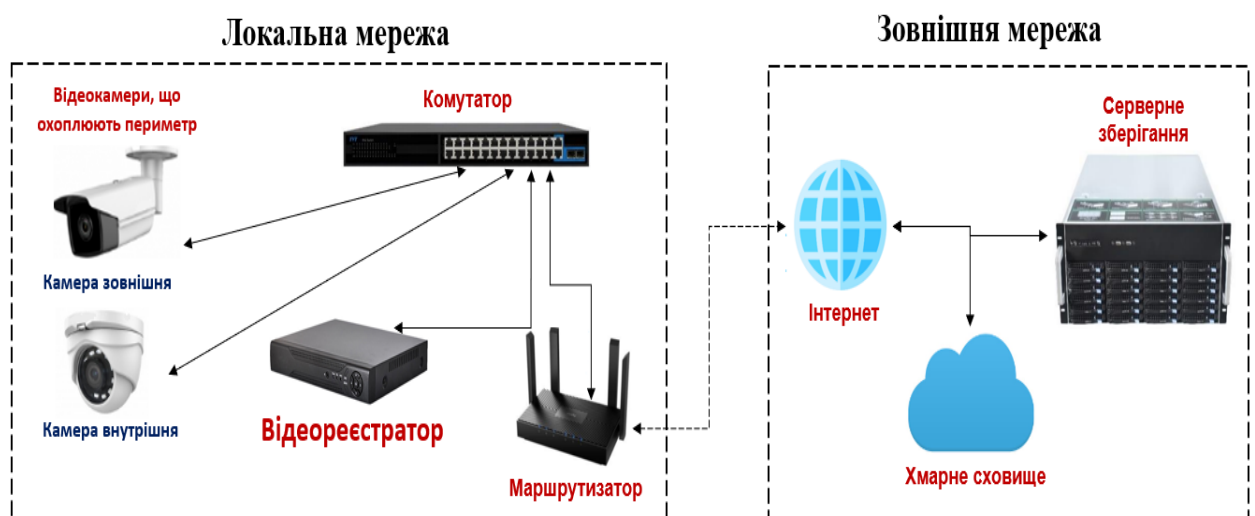


Рисунок 1.21 – Схема комутації відеоспостереження

Розглянемо різні типи відеокамер внутрішні/зовнішні для охорони стаціонарно видаленого об'єкта підвищеної захищеності:

1) Відеокамера Hikvision DS-2CD2423G2-I (2.8 мм) - це високоякісний пристрій відеоспостереження з роздільною здатністю 2 мегапікселі, призначений для використання в системах безпеки та нагляду будинків, квартир, магазинів, офісів і тд.



Рисунок 1.22 – Внутрішня IP камера Hikvision

Основні характеристики IP камери Hikvision:

- Роздільна здатність 2 мегапікселі (1920 x 1080 пікселів), така здатність відеокамери забезпечує високоякісне зображення.
- Є функція підключитися до мережі Ethernet або Wi-Fi, що дозволяє зручно встановлювати та керувати камерою через мережу.
- Камера має широкий кут огляду для охоплення великих просторів.
- Інфрачервоне підсвічування (до 30 метрів) для нічного бачення, що дозволяє отримувати чітке зображення навіть у темряві.
- Висока ступінь захисту від води та пилу за стандартом IP67, що дозволяє використовувати камеру в умовах зовнішнього середовища
- Підтримка різноманітних функцій безпеки та аналітики, таких як виявлення руху, перетин лінії, а також підтримка карт пам'яті для локального збереження відеозаписів.

2) Відеокамера Dahua DH-HAC-HFW1200CLP-IL-A – це камера зі спеціальним механізмом подвійного освітлення, яка забезпечує чітке та яскраве зображення у різних умовах. Камера має передові функції, що роблять її оптимальним вибором для нагляду за об'єктами, які потребують високого рівня безпеки. Однією з ключових особливостей даної камери є розумна система подвійного освітлення. Вона автоматично вмикає біле світло, коли функція захисту периметру/SMD Plus камери AI XVR виявляє об'єкт в зоні, відповідно до заданих правил. Це дозволяє отримувати чіткі та яскраві зображення цілей навіть при недостатньому освітленні. При виході об'єкта з

зони впливу, камера автоматично переходить на інфрачервоне освітлення. Це допомагає зменшити забруднення світла та забезпечує високоякісні зображення без впливу на оточуюче середовище.



Рисунок 1.23 – Відеокамера Dahua DH-HAC-HFW1200CLP-IL-A

Основні характеристики камери Dahua:

- Роздільна здатність 2 мегапікселі (1920 x 1080 пікселів), що забезпечує високоякісне зображення з деталізованими деталями.
- Технологія HDCVI, яка забезпечує передачу відеосигналу високої якості по коаксіальному кабелю на великі відстані без втрати якості.
- Інфрачервона підсвічування (до 30 метрів) для нічного бачення, що дозволяє отримувати чітке зображення навіть у темряві.
- Об'єктив з фокусною відстанню, який може бути вибраний залежно від потреб користувача, для забезпечення потрібного кута огляду.
- Корпус з металевого сплаву з високим ступенем захисту від води та пилу за стандартом IP67, що дозволяє використовувати камеру в умовах зовнішнього середовища.
- Широкі можливості налаштування параметрів зображення, таких як яскравість, контрастність, для досягнення оптимальної якості зображення.
- Підтримка різноманітних функцій безпеки та аналітики, таких як виявлення руху, перетин лінії, а також підтримка карт пам'яті для локального збереження відеозаписів.

1.3.8 Системи контролю доступу

Системи контролю доступу (СКД) - це комплексні охоронні рішення, спрямовані на контроль доступу осіб до певних приміщень та об'єктів. СКД включає в себе різноманітні пристрої, програмне забезпечення та технології, що дозволяють автоматизувати процеси ідентифікації користувачів. СКД забезпечують підвищену безпеку об'єктів, дозволяючи ефективно керувати доступом осіб за допомогою карток доступу, біометричних сканерів,

кодових замків тощо. СКД призначений для регулювання та обмеження доступу осіб до конкретних зон або приміщень. СКД може включати в себе захист об'єкту за допомогою карток, біометричні сканерів, PIN-коди тощо, також є можливість інтеграції з іншими системами для комплексного контролю.



Рисунок 1.24 – Ідентифікатори для СКД

Робота системи контролю доступом (СКД) відбувається за наступною схемою (Рисунок 1.25). Біля входу до обмеженого приміщення розміщуються пристрої-зчитувачі, які призначені для отримання інформації з ідентифікатора, введення пароля або коду, а також збору біометричних даних особи. Після цього зібрана інформація передається контролерам доступу, які, проаналізувавши дані про користувача, здійснюють керування різними пристроями: відкривають або блокують двері, активують сигнали тривоги, фіксують присутність особи на робочому місці та інше.



Рисунок 1.25 – Схема роботи СКД

Основні можливості системи контролю доступу (СКД):

- Управління доступом до певних приміщень лише авторизованим користувачам за допомогою різноманітних методів аутентифікації, таких як карти доступу, біометричні дані або пін-коди.
- Моніторинг присутності тобто можливість вести облік присутності осіб

в певних зонах або приміщеннях. Вона може фіксувати час входу та виходу користувачів, що дозволяє здійснювати контроль робочого часу.

- Забезпечення безпеки тобто СКД допомагає забезпечити безпеку об'єктів, а також конфіденційність інформації, а головне дозволяє вчасно виявляти несанкціонований доступ і реагувати на нього.

- Централізоване керування може бути з одного пункту, що спрощує управління доступом для всієї системи, а також забезпечує єдність політик безпеки.

1.4 Сучасні технології в охоронних системах

Сучасні технології в охоронних системах охоплюють широкий спектр інноваційних технологій, призначених для підвищення ефективності, безпеки та автоматизації заходів безпеки. Сучасні технології, що використовуються в охоронюваних системах:

- Відеоаналітика з використанням штучного інтелекту (ШІ) для аналізу записів з камер відеоспостереження. Така функція, як виявлення аномалій і розпізнавання об'єктів, використовуються для автоматичного спостереження і виявлення загроз.

- Системи біометричної ідентифікації дозволяє розпізнавати осіб за допомогою аналізу анатомічних ознак та поведінки (розпізнавання по голосу, відбитки пальців, сканування обличчя).

- Хмарні технології використовуються для зберігання та обробки даних у хмарних сервісах для збільшення та доступності інформації.

- Дрони та безпілотники використовуються для патрулювання, віддаленого спостереження та виявлення загроз.

1.5 Основні принципи роботи охоронних систем

Охоронна система – це елемент безпеки, що використовується на об'єктах для захисту від крадіжок. Основним компонентом охоронних систем є датчики, розміщені на дверях, вікнах, стінах та інших місцях на об'єкті. Вони можуть бути різних типів, від інфрачервоних датчиків руху до магнітних контактів. При виявленні загрози датчики надсилає тривожний сигнал до ППК.

Отже, основні принципи роботи охоронних систем полягають у:

- Виявлені загроз, тобто охоронні системи виявляють потенційні загрози за допомогою датчиків руху, розбиття скла, відеокамер і тд. Ці охоронні прилади можуть вказувати на можливе вторгнення на об'єкт або іншу загрозу.

- Сповіщення про проникнення на об'єкт, після виявлення загрози охороні прилади передають сигнал тривоги на ППК той у свою чергу передає тривожне сповіщення власнику на мобільний телефон та пульт централізованого спостереження.

2. Архітектура та технічні вимоги до охоронних систем

2.1 Архітектура охоронних систем

Мета архітектури охоронних систем створити ефективну та надійну інфраструктуру для захисту об'єкта та реагування на потенційні загрози. Добре продумана архітектура оптимізує продуктивність системи, підвищує ефективність, полегшує обслуговування і розширення, а також захищає від фізичних атак та потенційних кіберзагроз.

2.1.1 Централізована система керування

Централізована система керування – це програмне забезпечення (наприклад: Ajax Pro Desktop, Tiras oLoder), в якій усі функції керування охоронними приладами інтегровані в одну точку керування. Програмне забезпечення може бути встановлене на комп'ютер або телефон, з якого можливе керування різним доступ до будівлі, відеоспостереженням, виявлення вторгнення. Централізована система керування централізують систему та спрощують моніторинг за об'єктом.

2.1.2 Інтеграція охоронних систем

Мета інтеграції охоронних систем полягає у поєднанні різних видів охоронних систем, таких як відеоспостереження, системи контролю доступу (СКД) та охоронні прилади у єдину охоронну систему. Інтеграція систем безпеки дозволяє автоматизувати багато процесів, таких як виявлення вторгнень, моніторинг персоналу та інше. Це сприяє підвищенню ефективності та комплексності захисту об'єкта.

2.1.3 Системи комунікацій та зв'язку

Комунікаційні системи охоплюють технічні засоби, що забезпечують обмін даними за допомогою пристроїв між різними об'єктами. Вони включають різноманітні технології, такі як дротові та бездротові мережі, телефонію, Інтернет, мобільний зв'язок.

Основна мета комунікаційних систем полягає у забезпеченні ефективного обміну даними між користувачами та охоронними приладами у реальному часі (наприклад: передача повідомлень, текстових даних, зображень та відео).

2.2 Технічні вимоги до охоронних систем

Технічні вимоги повинні бути спрямовані на забезпечення надійної та ефективної роботи охоронних систем, та реагувати на потенційні загрози.

Основні технічні вимоги до охоронних систем – це наявність системи тривожної сигналізації (СТС) охоронні прилади реагують на вторгнення до

охоронюємого об'єкту та надсилають тривожне сповіщення на пункт централізованого спостереження, зв'язок (наявність засобів зв'язку важливе для передачі тривожних сповіщень на ПЦС), відеоспостереження (можливість запису відео в реальному часі), системи контролю доступу (постійний контроль доступу до об'єкту використовуючи брелоки, картки та інше) та резервне живлення для безперебійної роботи охоронних систем.

2.2.1 Надійність та стійкість

Для забезпечення надійності та стійкості рекомендується використовувати якісні охоронні прилади, регулярне технічне обслуговування охоронних приладів сприяють надійності та більшого терміну роботи.

Для забезпечення більшої стійкості потрібно виконувати заходи з кібербезпеки, такі як автентифікація, авторизація та шифрування даних. Також потрібно регулярно оновлювати ПЗ для усунення вразливих місць в охоронних системах.

Отже, надійність потрібна для безперебійної та ефективно роботи протягом тривалого періоду у складних умовах експлуатації. Стійкість потрібна витримування вплив кібератак.

2.3 Аналіз та управління ризиками в охоронних системах

По-перше, необхідно визначити потенційні загрози, які можуть негативно вплинути на об'єкт (втручання злочинців, кібератака та інше). Після виявлення загроз потрібно провести їхнє оцінювання на ймовірність проникнення. Після оцінки на ймовірність проникнення потрібно проаналізувати заходи на їх зниження (наприклад систематично оновлювати ПЗ). Критично важливо мати план дій у випадку надзвичайних ситуацій, таких як кібератаки або втручання підозрілих осіб на об'єкт.

3. Побудова автоматизованої системи охорони

Автоматизована система охорони – це комплексна система апаратного і програмного забезпечення, яка автоматизує охоронні дії захисту об'єкта. Автоматизована система охорони включає різноманітні компоненти, такі як охоронну сигналізацію, відеоспостереження, системи контролю доступу.

3.1 Огляд та аналіз об'єкту на потенційно небезпечні та вразливі місця

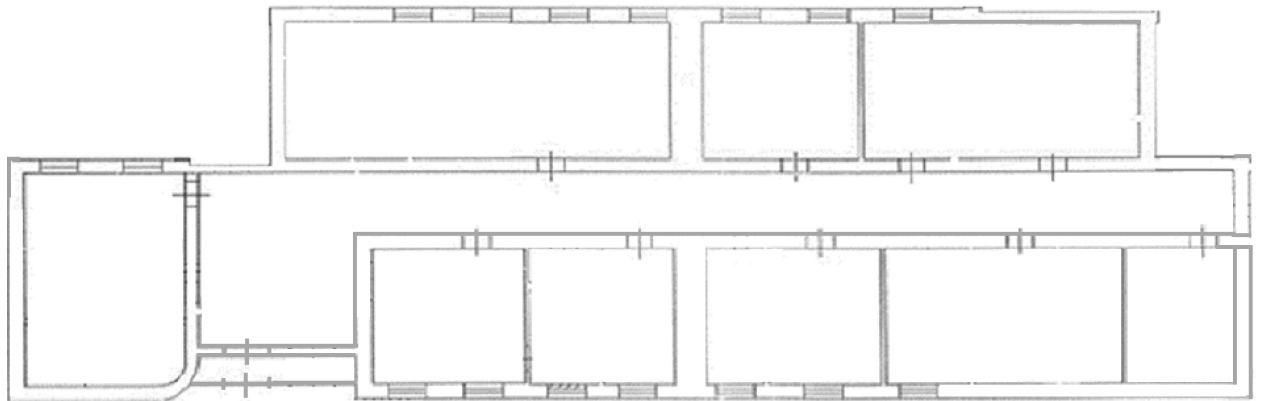


Рисунок 3.1 – Схема умовного об'єкта

На рисунку 3.1 зображена схема об'єкта який потрібно заблокувати охоронними приладами, відеонаглядом та системою контролю доступу. Перед тим як блокувати об'єкт потрібно оглянути схему та визначити всі основні зони та точки доступу до об'єкту які потребують блокування, потрібно ретельно оглянути кожну зону на можливість проникнення, особливо зосередити увагу на зонах з обмеженим доступом. Після огляду потрібно задокументувати де знаходяться проблемні зони об'єкта, потім потрібно вжити заходи та визначитися з місцем розташування охоронних приладів, відеокамер та системи контролю доступу для повного блокування щоб не було потенційно небезпечних та вразливих місць на віддаленому об'єкті підвищеної захищеності.

Таблиця 3.1 – Характеристики умовного об'єкту

Назва	Кількість
Вхід/Вихід	1
Коридор	1
Кімнат	9
Вікон	16

3.1.1 Аналіз можливих ситуацій на об'єкті

На віддаленому об'єкті підвищеної захищеності можливі потенційно небезпечні ситуації такі як:

- Розбиття скла задля вторгнення на об'єкт;
- Спрацювання сигналу «Тривога» на об'єкті;
- Знеструмлення об'єкту;
- Механічні впливи на об'єкт (удари молотом, свердління, вибухи тощо);
- Вторгнення на об'єкт осіб з метою вчинити злочин (крадіжка, вандалізм тощо);
- Напад на осіб які перебувають на об'єкті;
- Виникнення надзвичайної ситуації;
- Кібератака на охоронні прилади (є можливість втратити контроль над охоронним приладом, що може привести до відмови працездатності охоронних приладів та крадіжки цінних речей);

Задля запобігання таких ситуацій необхідно вживати наступні заходи, забезпечення об'єкту резервним живленням, всіма необхідними охоронними датчиками та вживати заходи щодо кібербезпеки регулярне оновлення програмного забезпечення виробників охоронних приладів, захист мережі, та використання надійних паролів).

3.2 Вибір охоронної сигналізації

Вибір системи охоронної сигналізації для охороняемого об'єкта визначається такими факторами як розмір об'єкта, функціональні можливості та бюджет для охоронної сигналізації.

Наприклад, для великого об'єкту може бути раціональна охоронна система з великою кількістю датчиків, відеоспостереженням, у той час як для невеликого об'єкту може бути раціональна більш проста охоронна система з базовим функціоналом. Важливо врахувати можливість майбутнього оновлення охоронної системи, тобто щоб була відповідність зростаючим потребам безпеки об'єкта.

Отже, на рисунку 3.1 зображена схема умовного об'єкту під який потрібно обрати охоронну сигналізацію (дротова/бездротова).

Вибір падає на бездротову охоронну сигналізацію Ajax яка одна з найсучасніших та найкращих охоронних систем на сучасному ринку. Цінова політика та якість матеріалів відповідають сучасним нормам. Бездротова охоронна сигналізація AJAX працює за допомогою двостороннього зв'язку (протокол Jeweller) та на частотному діапазоні 868,0 – 868,6 МГц або 868,7 – 869,2 МГц залежить від регіону.

Для блокування умовного об'єкту (рисунок 3.1) охоронною сигналізацією потрібні наступні прилади фірми Ajax.

Таблиця 3.2 – Список приладів для блокування об'єкту

Назва	Кількість
Прилад приймально-контрольний	1
Датчик руху	1
Комбінований датчик руху	10
Магнітно-контактний сповіщувач	26
Датчик розбиття скла	1
Клавіатура	1

3.2.1 Розміщення охоронних приладів на об'єкті

Розміщення охоронних приладів встановлюються за допомогою умовних позначення згідно ДСТУ 4030-2001. Список приладів які потрібні розмістити на схемі 3.1 зазначено в таблиці 3.2. Розташуванням охоронних приладів згідно ДСТУ 4030-2001 в Додатку Б.

Згідно додатку Б в кабінеті № 1 встановлено 1 комбінований датчик руху (так як датчик встановлений напроти вікон і у разі розбиття скла та рухів він спрацює) та 3 магнітно-контактних сповіщувачі (потрібен для виявлення несанкціонованого взлому дверей), в кабінеті № 2, 3 встановлено 1 комбінований датчик руху та 3 магнітно-контактних сповіщувачі, в кабінеті № 4 встановлено 1 комбінований датчик руху та 2 магнітно-контактних сповіщувачі, в кабінеті № 5 встановлено 1 комбінований датчик руху та 1 магнітно-контактний сповіщувач, в кабінеті № 6 встановлено 1 комбінований датчик руху та 3 магнітно-контактних сповіщувачі, в кабінеті № 7 встановлено 1 комбінований датчик руху та 3 магнітно-контактних сповіщувачі, в кабінеті № 8 встановлено 2 комбінованих датчиків руху та 5 магнітно-контактних сповіщувачі, в кабінеті № 9 встановлено 1 комбінований датчик руху та 3 магнітно-контактних сповіщувачі, в коридорі встановлений 1 прилад приймально-контрольний (встановлений по центру об'єкта для більш ефективного підключення радіо датчиків), 1 клавіатура (встановлення біля входу/виходу для зручного покидання об'єкта після поставлення об'єкта під сигналізацію), 1 датчик розбиття скла (встановлений біля входу/виходу для виявлення розбиття скла, так як входні двері скляні).

3.3 Вибір обладнання для відеонагляду

Вибір системи відеонагляду для охороняемого об'єкта визначається такими факторами як розмір об'єкта, функціональні можливості та бюджет.

Наприклад, для великого об'єкту може бути раціонально обрати відеонагляд з великою кількістю відеокамер, у той час як для невеликого об'єкту раціонально обрати більш прості відеокамери з базовим функціоналом. При виборі обладнання системи відеоспостереження необхідно визначитися з типом камери, у даному випадку згідно рисунку 3.1 потрібно

використовувати внутрішні (для приміщення) ІР камери з інфрачервоним підсвічування (до 30 м.) для нічного спостереження фірми Hikvision, камера має широкий кут огляду, функція підключення до мережі або Wi-Fi, роздільна здатність 1920 x 1080 пікселів.

Таблиця 3.3 – Список приладів для відеонагляду

Назва	Кількість
Внутрішня камера	3
Відеореєстратор DVR	1
Жорсткий диск на 5TB	1
Комутатор	1
Маршрутизатор	1
Автоматизоване робоче місце	1

3.3.1 Розміщення відеонагляду на об'єкті

Було розміщено відеокамери на об'єкті за допомогою вигаданих позначення. Список приладів для відеонагляду які потрібні розмістити на схемі 3.1 зазначено в таблиці 3.3. Розташовані відеокамери вигаданими позначеннями в Додатку В.

Згідно додатку В в кабінеті № 1 встановлено 1 автоматизоване робоче місце (для моніторингу за об'єктом, адміністрування та перегляду відеозаписів), 1 маршрутизатор (щоб була можливість підключатися до DVR через мережу), 1 комутатор (щоб була можливість більшого підключення відеокамер), 1 відеореєстратор DVR (щоб була можливість зберігати відеоматеріали та проводити постійний моніторинг за об'єктом у разі відсутності мережі (локально)), в коридорі встановлено 3 внутрішніх відеокамери Hikvision для постійного моніторингу за об'єктом.

3.4 Вибір системи контролю доступ (СКД)

Для умовного об'єкту (рисунок 3.1) потрібно обрати надійну і точну систему контролю доступу яка надає доступ до об'єкту за допомогою карток або брелків. Також потрібно обирати СКД з перспективою зростаючим потребам та спрощеним управлінням та адмініструванням. Головне для вищезазначеного умовного об'єкту це вартість. Отже спираючись на ціну та надійність системи контролю доступу, ідеальним варіантом буде турнікет, він забезпечує ефективний контроль доступу дозволяючи заходити лише авторизованим особам (та обмежити доступ не авторизованим). За допомогою турнікету можливо контролювати наявність/відсутність осіб на об'єкті.

Отже, для блокування умовного об'єкту (рисунок 3.1) системою контролю доступу потрібно наступні прилади.

Таблиця 3.4 – Список приладів для СКД

Назва	Кількість
Турнікет	1
Контролер	1
Кнопка відкриття турнікету	1
Автоматизоване робоче місце	1

Список приладів для системи контролю доступу які потрібні розмістити на схемі 3.1 зазначено в таблиці 3.4. Система контролю доступу розташована в Додатку Г вигаданими позначеннями.

Згідно додатку Г в кабінеті № 1 встановлено 1 автоматизоване робоче місце (для моніторингу та адміністрування системи контролю доступу), 1 контролер (щоб була можливість налаштовувати турнікет так як контролер є ключовою складовою системи контролю доступу і відповідає за керування турнікетом), 1 кнопка (для відкриття турнікету без картки або брелка), на вході до об'єкту встановлено 1 турнікет щоб не було несанкціонованого доступу.

4. Впровадження технологій безпеки на об'єкті або охорона праці

4.1 Визначення потенційно небезпечних виробничих факторів на об'єктів

Основними шкідливими та небезпечними факторами є:

1. Робота на ЕОМ (напруга органів зору і пов'язані з нею втому, хвороби, побічні ефекти, застійні явища в організмі через тривале перебування в одному положенні, причини різних захворювань, різні види випромінювання при використанні ЕПТ відеомоніторів, механічний шум, пов'язаний з роботою. електромеханічного друкуючого пристрою (принтера) і вентиляторів системи відводу тепла ЕОМ, наявність позитивних іонів, що виникають внаслідок іонізації повітря, елементами високовольтної схеми блоку живлення відеотерміналу).

2. Небезпечні значення напруги електромережі живлення, замикання якої може відбутися через тіло людини у випадку дотику до відкритих струмоведучих частин чи електроустаткування з порушеною ізоляцією.

3. Носіння, використання та застосування вогнепальної зброї та спецзасобів.

4. Ослаблення самоконтролю, переоцінка своїх сил і можливостей, невиправданий ризик.

5. Злочинні дії осіб, у відношенні працівника, з метою перешкоджання виконання ним обов'язків з охорони громадського порядку та боротьби зі злочинністю, заволодіння зброєю та спецзасобами.

6. Порушення Правил пожежної безпеки.

7. Концентрація небезпечних речовин у робочій зоні.

8. Порушення режиму праці/відпочинку.

9. Незадоволеність психологічним кліматом у колективі.

Процедура розслідування та облік нещасних випадків і професійних захворювань та катастроф:

1. Кожен інцидент, що стався, підлягає розслідуванню протягом певного періоду часу комісією під головуванням керівника відділу охорони праці та безпеки життєдіяльності.

2. Потерпілий або працівник чи інша особа, якій стало відомо про нещасний випадок, повинен негайно повідомити свого керівника і вжити заходів для надання потерпілому необхідної допомоги.

3. Протягом одного дня після завершення розслідування керівник підтверджує ці дії та надає копію потерпілому на підпис.

4. Про кожний інцидент слід повідомляти безпосередньому керівнику або вищому керівництву співробітника, який виявив інцидент, або самому потерпілому, а також слід вжити заходів для забезпечення лікування в лікарні.

5. Перелік обставин, за яких настає страховий випадок державного соціального страхування громадян від нещасного випадку на виробництві та професійного захворювання:

1) Потерпілий виконує свої трудові (службові) обов'язки згідно з графіком роботи, та у відрядженнях.

2) Перебування особи на АРМ, на об'єкті або в будь-якому іншому місці, пов'язаному з виконанням трудових обов'язків або адміністративних завдань, з моменту прибуття до моменту відходу. Це має бути зафіксовано відповідно до внутрішнього розпорядку, включаючи робочий час та понаднормові години;

3) Підготовка до роботи та прибирання після роботи інструменту, засоби захисту, одяг, заходи особистої гігієни, пересування територією до та після роботи;

4) Потерпілий подорожує до або з будь-якої установи (між установами), що обслуговується, за затвердженим маршрутом;

5) Пересування до місця роботи та з місця роботи особи відповідно до визначених завдань, включаючи всі види та форми транспорту, що перебувають у власності жертви;

6) Інше ушкодження здоров'я потерпілого внаслідок погіршення стану здоров'я внаслідок впливу небезпечних виробничих факторів або навколишнього середовища під час виконання службових обов'язків (роботи) підтверджується медичною довідкою.

7) Вплив небезпечних або шкідливих виробничих факторів на роботі та/або раптове погіршення стану здоров'я внаслідок важкості або напруженості трудового процесу, що підтверджено медичним висновком, або потерпілий не пройшов медичний огляд у встановленому законодавством порядку і медичний висновок про стан його здоров'я свідчить про те, що робота, яка виконується, протипоказана даній особі;

8) Вплив на потерпілого шкідливих або небезпечних виробничих факторів, що призвів до встановлення діагнозу професійного захворювання.

6. Ситуації, коли нещасний випадок не може бути пов'язаний з роботою, такі:

1) Проживання в постійному поселенні на території польового або вахтового табору;

2) Використання транспортних засобів, обладнання, інструментів та матеріалів в особистих цілях;

3) Вживання алкоголю, наркотиків, токсичних речовин і отрут та погіршення стану здоров'я через їх впливу (наприклад, утоплення, параліч, зупинка серця).

Це не застосовується, якщо нещасний випадок пов'язаний з використанням таких речовин у виробничому процесі або з порушенням вимог щодо їх зберігання та транспортування, або якщо потерпілий у стані алкогольного, токсичного чи наркотичного сп'яніння був відсторонений від роботи до настання нещасного випадку відповідно до вимог правил внутрішнього трудового розпорядку.

4) Алкогольні сп'яніння, отруєння та наркотичні інтоксикації, не пов'язані з виробничим процесом, є основною причиною нещасного випадку, підтвердженою відповідною медичною довідкою, коли немає технічних або організаційних причин для настання нещасного випадку;

5) Вчинення злочину, підтверджене обвинувальний вирок або рішення про закриття кримінального провадження (кримінальне) з nereабілітуючих підстав;

6) смерть від природних причин, смерть від загального захворювання або самогубство (крім випадків, передбачених пунктом 5 статті 8 цього Порядку), підтверджена результатами судово-медичної експертизи та/або відповідною постановою про закінчення кримінального провадження.

7. Масові нещасні випадки (за участю двох і більше працівників одночасно) та нещасні випадки зі смертельними наслідками підлягають спеціальному розслідуванню протягом 10 робочих днів комісією під головуванням представника відповідного органу Держгірпромнагляду.

8. Розслідуванню підлягають усі вперше виявлені хронічні професійні захворювання та отруєння.

4.2 Засоби індивідуального захисту та перша медична допомога

«ЗІЗ» засоби індивідуального захисту - це низка засобів, призначених для забезпечення безпеки людей у різних небезпечних або потенційно травматичних ситуаціях. Ось деякі з найпоширеніших ЗІЗ:

1. Одяг і взуття: спеціалізований одяг і взуття, призначені для захисту від механічних пошкоджень, хімічних речовин, екстремальних температур та ураження електричним струмом. Такий одяг включає в себе захисний одяг, рукавички, шоломи та спеціалізоване взуття.

2. Окуляри і маски: використовуються для захисту очей і дихальних шляхів від пилу, різних хімікатів, волокон і токсичних газів. Існують різні типи окулярів і масок, які підбираються відповідно до умов роботи.

3. Засоби захисту органів слуху використовуються для захисту вух від шуму та високочастотних звуків, які можуть спричинити втрату слуху. Можна використовувати спеціальні навушники або беруші.

4. Респіратори та фільтри для захисту дихальних шляхів від шкідливих речовин, що переносяться повітрям, таких як пил, дим, пари розчинників і токсичних газів. Респіратори мають різні рівні захисту залежно від типу фільтра.

5. Засоби самозахисту, включаючи огорожі, бар'єри, сигналізацію та інші пристрої, які допомагають уникнути або швидко виявити потенційно небезпечні ситуації.

6. засоби захисту від ударів і падінь, включаючи низку пристроїв, що запобігають падінню і травмам від ударів, такі як ремені безпеки, спеціальні системи безпеки і подушки.

Перша допомога:

1. 1-ша допомога - це комплекс заходів, що вживаються родичами потерпілого (взаємодопомога) або самим потерпілим (самодопомога) з метою відновлення або збереження життя і стан здоров'я потерпілого до прибуття в медичний заклад. персонал

2. Перша допомога при пораненнях:

1) Насамперед зупиніть кровотечу і накладіть на рану стерильну пов'язку. Кровотечу в кінцівці слід зупинити, притиснувши артерію, вену або джгут до рани (піднявши кінцівку);

2) Якщо використовується джгут (якщо його немає, використовуйте ремінь, пояс, мотузку, розірвану сорочку тощо), обмотайте ділянку, на яку накладається пов'язка, шматком тканини, щоб запобігти болю;

3) Джгут не слід носити більше 1-2 годин. У зв'язку з цим під джгутом або на кінцівці слід зробити позначку чорнилом або хімічною ручкою про те, коли саме був накладений джгут. Після зупинки кровотечі обробіть продезінфікуйте шкіру навколо рани спиртом, нанесіть йод або зеленку і накладіть стерильну пов'язку.

3. Перша допомога при переломах:

1) При лікуванні переломів будьте обережні, щоб закритий перелом не перетворився на відкритий;

2) При відкритих переломах спочатку накладіть стерильну пов'язку та іммобілізуйте кінцівку, як описано вище;

3) Накласти на кінцівку шину, дошку або стержень і забинтувати її так, щоб шина охопила два найближчі суглоби і не давала їм рухатися; 4) Накласти на кінцівку шину, дошку або стержень і забинтувати її так, щоб шина охопила два найближчі суглоби і не давала їм рухатися; 5) Накласти на кінцівку шину, дошку або стержень і забинтувати її так, щоб шина охопила два найближчі суглоби і не давала їм рухатися.

4. Перша допомога при вивихах, ударах і розтягненнях:

1) До таких ускладнень відносяться, травми. Тому постраждалих з травмами черепа необхідно покласти на холодну поверхню (сніг або лід) з піднятою головою і доставити в лікарню;

2) Вивих викликає біль і зміну форми суглоба. Перша допомога при вивиху - накласти пов'язку, щоб запобігти руху суглоба, і негайно доставити до лікарні;

3) Розтягнення зв'язок викликає гострий біль і набряк суглоба. Перша допомога полягає в накладенні пов'язки на пошкоджену ділянку і транспортуванні в лікарню.

5. Перша допомога при опіках:

1) Залежно від характеру впливу, опіки можуть бути термічні опіки (від вогню, гарячого металу або води), хімічні опіки (від кислот і лугів), електричні опіки та променеві опіки (від ультрафіолетового або інфрачервоного випромінювання);

(2) Залежно від ступеня впливу, опіки бувають наступними:

- Перший ступінь: почервоніння та біль;
- Другий ступінь: утворення пухирів на шкірі;
- Третій ступінь: некроз поверхневих або глибоких шарів шкіри;
- Четвертий ступінь: некротичні тканини під шкірою;

3) При наданні першої допомоги при опіках в першу чергу слід усунути причину опіку;

4) Зніміть з потерпілого непотрібні предмети або речі (наприклад,

годинник, одяг, ланцюжки, браслети). Одяг, що прилип до опіку, слід розрізати;

5) При опіках першого та другого ступенів необхідно охолодити рану під проточною водою. Охолодіть місце опіку під проточною водою. Через 10-15 хвилин накласти вологу пов'язку;

6) Якщо опік більш важкий, опік третього або четвертого ступеня, обмотайте місце опіку чистим вологим бинтом, наповніть відповідну ємність холодною водою, помістіть в неї забинтовану ділянку опіку і почекайте деякий час;

7) Відправте потерпілого в лікарню;

8) При опіках забороняється наступне

- При опіках не наносити крем, олію або мазь на місце опіку;

- Зривати одяг, що прилип до опіку; 9) Розірвати одяг, який прилип до опіку; 10) Розірвати одяг, який прилип до опіку.

- Проколоти пухир.

6. перша допомога при обмороженні

1) Перші ознаки обмороження з'являються на незахищених ділянках тіла (руки, обличчя, ніс, вуха). Спочатку виникає відчуття холоду, поколювання і легкий біль, потім уражена ділянка шкіри починає бліднути і розвивається оніміння в ураженій ділянці;

2) Перша допомога при обмороженні полягає в розтиранні ураженої ділянки м'якими рукавичками або руками, поки ділянка не почервоніє і не стане теплою. Потім кінцівку слід занурити у воду ($36-37^{\circ}\text{C}$), обмотати стерильним бинтом і доставити в лікарню;

3) Нанесіть олію на відкриті ділянки тіла і тримайте шкіру в теплі, щоб запобігти обмороженню;

4) Обмороження можливе при дуже низьких температурах або при сильному вітрі. Першими симптомами обмороження є втома, ослаблення серцевої діяльності та дихання, сонливість і втрата свідомості, що може призвести до смерті;

5) Якщо необхідно надати першу допомогу, негайно віднесіть обмороженого в приміщення.

($36-37^{\circ}\text{C}$), зробіть штучне дихання, розітріть все тіло і дайте потерпілому стимулюючий засіб, наприклад, гарячий чай, каву або вино.

7. Перша допомога при ураженні струмом:

(1) При ураженні електричним струмом можлива втрата свідомості, судоми, серцева слабкість, зупинка дихання і смерть. У незначних випадках можуть виникнути опіки в місці контакту з електричними проводами;

2) Перед тим, як надати першу допомогу, потерпілого необхідно відокремити від дії електричного струму. Для цього вдягніть діелектричні калоші чи рукавички або обмотайте руки сухою тканиною чи сорочкою. Встаньте на суху дошку і використовуйте суху палицю або непровідну гуму, щоб одяг не потрапляв під струм.

8. Перша допомога при зупинці дихання та серця

1) Якщо відсутні життєво важливі ознаки (дихання, серцебиття, пульс),

пацієнт не реагує на больові подразники, а зіниці розширені і не реагують на світло, пацієнт вважається клінічно мертвим і слід негайно розпочати штучну вентиляцію легенів та зовнішній (непрямий) масаж серця;

2) Перед початком штучної вентиляції легень розстебнути комірці, послабити краватки і шарфи, розстебнути ремені, очистити ротову порожнину пальцями, обгорнутими бинтом або носовою хусткою, якщо в ній є сторонні тіла, кров, слиз або вибиті зуби, і повернути голову набік; якщо рот щільно закритий, помістити чотири пальці обох рук за кути щелепи, великі пальці з боків нижньої щелепи і розсунути щелепу так, щоб зуби нижньої щелепи опинилися попереду зубів верхньої щелепи;

3) Найефективнішим методом штучної вентиляції легенів є вентиляція "рот в рот". Повітря нагнітається в рот і ніс через марлю, серветку або хустинку так, щоб грудна клітка повністю роздувалася при кожному видиху. Швидкість видиху.

8-24 вдихи на хвилину. наприклад, не залишайте потерпілого на вологій або холодній підлозі. Підкладіть під потерпілого щось тепле і накрийте його/її. Як тільки дихання потерпілого відновиться, поновіть штучне дихання і переконайтеся, що подача повітря відповідає власному диханню потерпілого. Вентилюйте штучні легені до тих пір, поки потерпілий не прийде до тями або поки не будуть помічені незаперечні ознаки смерті;

4) За відсутності пульсу одночасно зі штучною вентиляцією легень проводити зовнішній (непрямий) масаж серця, який полягає в ритмічному стискання серця між грудиною та хребтом. При виконанні зовнішнього масажу серця переконайтеся, що потерпілий лежить на спині та на твердій поверхні (землі, ґрунті). Стоячи поруч з потерпілим, долоні рук слід притиснути один до одного з силою, яка прогинає грудину на 4-5 см у бік хребта (60-70 натискань за хвилину). Долоні слід покласти на нижню третину грудини, на два пальці вище мечоподібного відростка.

4.3 Професійна підготовка та навчання працівників з питань охорони праці

Перед початком роботи на драбинах, вимоги безпеки перед початком роботи

1) Одягніть робочий одяг, затягніть манжети і приберіть вільні кінці;

2) Освітлити робочу зону, усунути перешкоди для роботи та звільнити проходи;

3) Переконайтеся, що в робочій сумці знаходяться необхідні інструменти та обладнання; перевірити, що робоча сумка заповнена необхідними інструментами та обладнанням; підготувати і надіти страхувальний пояс, якщо ви працюєте на висоті понад 1,3 м; переконайтеся, що робоча зона добре освітлена і вільна від перешкод; переконайтеся, що в робочій сумці знаходяться необхідні інструменти та обладнання 1,3 м.

4) Перевірте наступний термін випробування зубила (долота);

5) Ретельно огляньте волокуші (драги) на предмет механічних

пошкоджень;

6) Забезпечити стійкість драбини (стрем'янки) і переконатися шляхом огляду та випробування, що драбина не ковзає і не рухається несподівано; і

7) Драбини повинні бути в хорошому стані, а сходинки повинні бути закріплені балками, а не прибиті цвяхами.

8) На сходинках не повинно бути тріщин або відколів, а на косоурах повинні бути верхні та нижні з'єднувальні болти.

9) Для запобігання ковзанню на підлозі драбина повинна мати гумові башмаки або загострені металеві наконечники на обох кінцях (драбини повинні бути випробувані статичним навантаженням).

Вимоги безпеки при роботі з драбинами:

1. Працювати з електроінструментом дозволяється тільки з драбини (стрем'янки), що має верхній настил з поручнями

2. При неможливості надійного закріплення верхньої частини драбини, а також при роботі в місцях з інтенсивним пішохідним рухом або на драбинах (стрем'янках) висотою більше 4 м, якщо на кінці тягової лінії (драбини) є металеві кінці або гумові башмаки, поблизу повинні знаходитися працівники для спостереження за робочою зоною і пересуванням людей, а тягову лінію (драбину) тягової лінії (стрем'янки) слід підпирати.

3. Якщо збирач вишні повинен контактувати з вхідними дверима, біля них повинен знаходитися працівник, щоб захистити їх від удару.

4. Для роботи на майданчику можна використовувати укорочену мотузку драбину або передбачити спеціальний настил.

5. При виконанні робіт на висоті, що перевищує 5,1,3 м, дозволяється передавати інструмент, пристосування та змінні блоки до працівника та від нього.

6. Під час роботи з ручних драбин або трапів забороняється:

1) Користуватися буксирними канатами, що не пройшли регулярний огляд;

2) Працювати з несправною драбиною; і

3) Стояти або ходити під драбиною, коли на ній знаходиться людина

4) Ставати на драбину на відстані менше 1 метра від верхньої частини драбини; працювати на недостатньо довгій драбині.

5) Якщо драбина недостатньо довга, організувати опорну конструкцію, наприклад, ящик або бочку, встановити переносну драбину під кутом не менше 75 градусів, без додаткового закріплення верхньої частини драбини; 6)

Якщо сходи недостатньо довгі, встановити переносну драбину під кутом не менше 75 градусів, без додаткового закріплення верхньої частини драбини

6) робота на двох верхніх сходинках сходів без поручнів;

7) перебування на драбині більше однієї особи; та

8) роботи з монтажу проводів і кабелів; роботи з монтажу проводів і кабелів; роботи з монтажу проводів і кабелів.

9) Робота з електроінструментами з приставної драбини; робота з електроінструментами з приставної драбини;

10) Підтримувати важкі компоненти на висоті;

11) Користуватися драбинами і плоскогубцями з металевими прутами під час виконання робіт з технічного обслуговування і ремонту електроустановок, а також під час заміни електроламп, крім випадків, зазначених у пункті 7 глави 1 цієї Інструкції

12) Використання замість драбин тимчасового підлогового покриття з довільними опорами (ящики, цегла тощо)

13) Використання замість врізання сходинок у мотузку пазів (klinів) зі сходинками, закріпленими цвяхами.

Вимоги безпеки при роботі з ручними інструментами.

1. Перед початком роботи

1) Переконайтеся, що робота придатна для ремонту; одягніть спецодяг, взуття та інші засоби індивідуального захисту;

2) Переконайтеся, що інструменти, необхідні для роботи, є в наявності та придатні до використання; і

3) Підготуйте робочу зону і розташуйте робоче обладнання та інструменти так, щоб вони не переміщувалися надмірно; і

4) Забезпечити достатнє освітлення робочої зони та наявність первинних засобів пожежогасіння; 4) забезпечити достатнє освітлення робочої зони та наявність первинних засобів пожежогасіння.

2) Не приступати до роботи до усунення виявлених порушень або дефектів.

Вимоги безпеки при використанні ручного інструменту.

1. При виконанні робіт ручним інструментом необхідно виконувати наступне

1) Одягати захисні окуляри, щоб запобігти потраплянню в очі твердих осколків, що вилітають від ударних інструментів;

2) при роботі з листовим металом використовувати брезентові рукавиці для запобігання травмуванню рук

3) Використовуйте захисні екрани (сітки) під час різання. Зменшуйте силу удару перед завершенням різання, щоб запобігти зісковзуванню металевих частин і зубила та травмуванню;

4) При використанні клинів або зубил з кувалдою використовуйте клинотримач з довжиною ручки не менше 0,7 м;

5) Використовуйте кільце при роботі з кліщами. Розмір кільця повинен відповідати розміру оброблюваної заготовки;

6) Використовуйте викрутку з шириною робочої частини (леза), що відповідає розміру паза в головці гвинта або болта;

7) Використовуйте гайковий ключ, у якого устя (рукоятка) не перевищує розмір головки болта (поверхні гайки) більш ніж на 0,3 мм; і

8) Розташовуйте електроінструмент так, щоб він не міг скотитися або впасти в робочу зону. Не розміщуйте електроінструмент поблизу перил, відкритих люків або шахт;

9) Під час нанесення розмітки слідкуйте за тим, щоб не порізатися гострими краями стріли або листового металу;

10) Під час різання металу покладіть пальці лівої руки на напилок;

11) Під час kleпання слідкуйте за робочою частиною інструменту і тримайте опору, але не надто міцно;

12) Зчищайте стружку щіткою і не дмухайте на неї (при дмуханні вона може потрапити в очі);

13) При роботі або транспортуванні інструментів з гострими краями ці частини повинні бути захищені.

Вимоги безпеки після закінчення роботи з ручним інструментом

1. Після закінчення робочого дня потрібно прибрати АРМ, зібрати інструменти та покласти їх на свої місця або здати на склад

2. Виносити виробничі відходи, сміття та невикористані матеріали у спеціально відведене місце

3. Упорядковувати та прибрати спецодяг та інші засоби індивідуального захисту, які використовувались під час роботи, у спеціально відведене для цього місце

4. Повідомляти найближчого керівника про виявлені під час дослідження недоліки в роботі.

5. Після закінчення роботи вимити руки з милом.

Правила користування електроінструментом, під час користування електроінструментом дотримуйтесь наступних правил, щоб уникнути ураження електричним струмом:

1. Використовуйте електроінструменти з 3-полюсним шнуром живлення із заземлюючим (нульовим) проводом, увімкненим першим.

2. Не вмикайте в мережу електроприлади з пошкодженими шнурами живлення.

3. Не підключайте прилади, штепсельна вилка, розетка або подовжувач яких ненадійно приєднані до електромережі.

4. Не вмикайте електроінструменти в розетки без захисних кожухів.

5. Не користуйтеся електричними лампами, у яких пошкоджені штепсельні розетки, з'єднувальні коробки, інші електроприлади або скло яких має ознаки потемніння чи здуття.

6. Не можна використовувати саморобні подовжувачі, які не відповідають вимогам Правил улаштування електроустановок (ПУЕ) для переносних електричних кабелів.

7. Не використовуйте для обігріву неякісні (саморобні) електронагрівальні прилади або лампи розжарювання

8. Якщо використовується пристрій з окремим (незалежним) заземлюючим провідником, перед підключенням пристрою до електромережі перевірте наявність і надійність заземлюючого провідника, підключеного до відповідної клема.

9. По можливості не торкайтеся руками металевих частин приладу, підключеного до електромережі

10. Не торкайтеся руками від'єднаних або оголених шнурів живлення.

11. Не замінюйте пошкоджені запобіжники або лампочки, не ремонтуйте прилад або шнури живлення.

12. Завжди відключайте прилад від електромережі, коли витираєте з нього

пил, має холодильник або підлогу біля нього.

13. Не залишайте прилад без нагляду під час роботи.

14. Після закінчення роботи вимикайте прилад і виймайте вилку шнура живлення з розетки.

15. При відключенні приладу від мережі не тягніть за шнур живлення, а тримайте прилад за корпус.

Дії працівника в разі ураження електричним струмом:

1. Перед наданням першої допомоги потерпілого необхідно відключити струм. Для цього надіньте діелектричні калоші та рукавички або обмотайте руки сухою тканиною, сорочкою тощо. Станьте на суху дошку і за допомогою сухої палиці або неструмопровідної шини відтягніть потерпілого від струму та звільніть його від дії струму, перев'язавши.

2. Якщо ознаки життєдіяльності (дихання, серцебиття, пульс) відсутні, пацієнт не реагує на больові подразники, а зіниці розширені і не реагують на світло, пацієнт вважається клінічно мертвим і слід негайно розпочати штучну вентиляцію легень та зовнішній (непрямий) масаж серця:

1) Перед початком штучної вентиляції легень розстебнути комір, розв'язати краватки і шарфи, розстебнути реміні, очистити рот пальцями, обгорнутими бинтом або носовою хусткою, якщо він наповнений сторонніми предметами, кров'ю, слизом або вибитими зубами, і повернути голову набік; якщо рот щільно закритий, покласти чотири пальці обох рук на нижню щелепу; великі пальці рук покласти за кути нижньої щелепи з боків нижньої щелепи і розсунути її так, щоб зуби нижньої щелепи опинилися перед зубами верхньої

2) Найефективнішим методом штучної вентиляції легень є вентиляція "рот в рот". Повітря нагнітається в рот і ніс через марлю, серветки або носові хустинки так, щоб грудна клітка повністю роздувалася при кожному видиху. Частота видихів.

8-24 видихів на хвилину. Це означає, що потерпілого не можна залишати на вологій землі або холодній підлозі. Підкладіть під потерпілого щось тепле і накрийте його/її. Як тільки дихання потерпілого відновиться, поновіть штучне дихання і переконайтеся, що вентиляція відповідає власному диханню потерпілого. Вентилуйте штучні легені до тих пір, поки потерпілий не прийде до тями або поки не будуть помічені незаперечні ознаки біологічної смерті;

3) За відсутності пульсу виконати екстракорпоральну (непрямую) СЛР, яка полягає у ритмічному стисканні серця між грудиною та хребтом одночасно зі штучною вентиляцією легень. При виконанні екстракорпоральної СЛР покладіть потерпілого на спину на тверду поверхню (землю, ґрунт). Стоячи поруч з потерпілим, долоні рук слід притиснути один до одного з силою, яка згинає грудику на 4-5 см у напрямку до хребта (60-70 натискань на хвилину). Долоні повинні бути розміщені на нижній третині грудини, на два пальці вище мечоподібного відростка.

3. Якщо у потерпілого є опік, обережно обмотайте пошкоджену ділянку стерильною пов'язкою, не торкаючись місця опіку, і транспортуйте до медичного закладу.

4.4 Організація навчання та перевірка знань з охорони праці

Навчання та інформаційні тести:

1. Працівники повинні бути проінформовані, навчені та протестовані як під час прийому на роботу, так і на робочому місці з питань охорони праці, надання першої медичної допомоги потерпілим та правил поведінки у випадку нещасного випадку.

2. Навчання та перевірка знань працівників з питань охорони праці та безпеки життєдіяльності, включаючи професійне навчання, перепідготовку та підвищення кваліфікації, здійснюється працівниками служби підтримки персоналу або іншими працівниками, призначеними керівництвом ТЕ для виконання цього завдання.

3. Перед перевіркою знань з охорони праці для працівників повинно бути організовано навчання, у тому числі лекції, семінари та консультації.

4. Перевірка знань з охорони праці та безпеки працівників повинна проводитися відповідно до нормативно-правових актів охорони праці, дотримання яких входить до посадових обов'язків працівника.

5. Працівники, у тому числі персонал, які не пройшли навчання, інструктаж і перевірку знань з питань охорони праці, до роботи не допускаються.

4.5 Вимоги безпеки в аварійних ситуаціях

1. негайно припинити роботу, відійти від небезпечної зони і вжити заходів щодо запобігання поширенню аварії (вимкнути загальний рубильник або автоматичний вимикач в електрощитовій установці для відключення електроенергії, а в разі пожежі або вентиляції вжити заходів щодо недопущення в місце аварії сторонніх осіб, крім зацікавлених осіб);

2. негайно відключити електрообладнання від електромережі в наступних випадках

- запаху диму, що виходить від електрообладнання; 3. іскріння від електрообладнання

- Іскріння на електрообладнанні;

- Виявлено наявність напруги на металевих частинах обладнання; 3;

- Відсутність напруги в електромережі;

- При виявленні несправності в системі вмикання/вимикання; - При виявленні несправності в системі вмикання/вимикання; - При виявленні несправності в системі вмикання/вимикання;

- Травмування працівника або іншої особи внаслідок ураження електричним струмом;

4.6 Робота з електроінструментами

Вимоги безпеки при роботі з електроінструментом.

1. Перед початком роботи:

- 1) Одягніть робочий одяг;
- 2) За необхідності забезпечте себе спеціальними антивібраційними рукавичками (м'якими, з подвійною підкладкою), захисними окулярами (окуляри з небитким склом) тощо;

- 3) Огляньте робочу зону, усуньте перешкоди для роботи та розчистіть коридори.

2. Залежно від характеру роботи, необхідно зробити наступне:

- 1) Переконайтеся, що тип і клас електроінструментів (як зазначено) відповідають типу роботи, що виконується

- 2) Використовувати захисні окуляри та спеціальні антивібраційні рукавички під час роботи з ударними інструментами; і

- 3) Затягнути манжети та закріпити кінці одягу, що звисають, під час роботи з інструментами з частинами, що обертаються; 4) носити захисні окуляри та спеціальні антивібраційні рукавички під час роботи з ударними інструментами; та

- 3) Переконайтеся, що робоча зона добре освітлена, за необхідності використовуйте переносний електричний ліхтар. Переконайтеся, що переносний світильник обладнаний захисною сіткою зі світловідбивачами та гачком для підвішування, а його кабелі справні.

4. Перевірте затягування гвинтів кріплення вузлів і деталей електроінструменту, стан кабелів, відсутність зовнішніх пошкоджень або обривів проводів, справність вимикача і заземлення, а також роботу електроінструменту на холостому ході. У цьому випадку підключайте електроінструмент до електромережі тільки з вимикачем у положенні "вимкнено".

Наступні несправності є неприпустимими:

- 1) Пошкодження штепсельного з'єднання, кабелю живлення (шнура) або його ізоляції;

- 2) Несправність вимикачів; - несправність мережевого кабелю (шнура); - несправність вимикача

- 3) Пошкодження кришки щіткотримача;

- 4) Тріщини або інші пошкодження, що знижують міцність блоку або ручки; тріщини або інші пошкодження, що знижують міцність блоку або ручки; пошкодження редуктора або вентиляційної коробки

- 5) Витік масла з редуктора або вентиляційних каналів; пошкодження кришки щіткотримача; пошкодження кришки щіткотримача; пошкодження кришки щіткотримача

5. По можливості підвісьте кабель живлення електроінструменту. Якщо кабель прокладений на підлозі, його необхідно захистити від механічних пошкоджень: накрити, обгородити, повісити попереджувальні знаки.

Забороняється прямий контакт кабелю з металевими, гарячими, вологими або масляними поверхнями при роботі з електродрилем виріб, що свердлиться, повинен бути надійно закріплений.

Вимоги безпеки при використанні електроінструментів:

1. У разі раптової зупинки (наприклад, відключення електроенергії,

заклинювання рухомих частин) негайно вимкніть електроінструмент вимикачем.

2. Від'єднайте електроінструмент від мережі:

1) Якщо робота перервана;
2) При переміщенні інструменту з однієї робочої зони в іншу; 3) при переміщенні інструменту з однієї робочої зони в іншу; 4) при переміщенні інструменту з однієї робочої зони в іншу

3) Коли працівник відсутній на робочому місці; та

4) В кінці роботи або в кінці робочого дня; 5) коли корпус інструменту дуже гарячий

5) Коли корпус інструменту занадто гарячий; 6) при виявленні слабкого струму

6) При виявленні слабкого струму;

7) Коли вимикач вийшов з ладу;

3. При виявленні несправності електроінструменту, перегріву корпусу інструменту або ослаблення струму після відключення від електромережі повідомити керівника робіт (безпосереднього керівника) про необхідність заміни електроінструменту і відправити несправний електроінструмент на перевірку (ремонт).

4. при роботі з електродрилем очищайте металеві частини спеціальним гачком або щіткою після зупинки електродриля.

5. Встановлюйте і закріплюйте оброблювану деталь так, щоб вона не зісковзувала в робочі години.

Вимоги безпеки після закінчення роботи з електроінструментом:

1. Вимкніть електроінструмент вимикачем, від'єднайте мережевий шнур від електромережі та вийміть робочий інструмент з патрона електроінструменту.

2. При необхідності проведіть профілактичне обслуговування електроінструменту відповідно до інструкції з експлуатації.

3. Утримуйте робочу зону в чистоті.

4. Поверніть електроінструмент або зберігайте його в безпечному місці.

Під час користування електроприладами заборонено виконувати такі дії:

1) Використання транспортних засобів, які не відповідають поставленим завданням; і

2) Заземлення електроприладів II і III класу; 3) використання інструменту, що не відповідає його паспорту; 4) використання інструменту, що не відповідає його паспорту; та

3) Перевищення терміну безперервного використання, зазначеного в паспорті транспортного засобу; та

4) Передавати інструмент, навіть на короткий час, іншій особі, яка не має права працювати з електроінструментом; використовувати інструмент не за призначенням.

5) Торкатися ріжучих або обертових частин інструменту;

6) Триматися за шнур електроінструменту;

7) Ручне видалення тирси або стружки;

- 8) Робота з драбиною, що входить до комплекту поставки;
 - 9) Транспортування замерзлих або мокрих дерев'яних частин;
 - 10) Тягнути або скручувати кабелі електроінструментів;
 - 11) Перехрещення кабелю живлення електроінструменту з іншими кабелями або шнурами;
 - 12) Охолодження корпусу електроінструменту снігом або водою в разі його перегріву
 - 13) Продовжувати роботу, якщо з'явився характерний дим або запах горілої ізоляції, круговий вогонь в колекторі через підвищене іскріння щіток, підвищений шум, стукіт, вібрація або пошкодження робочого інструменту.
- Запобіжні заходи в аварійних ситуаціях:
1. Під час використання електроінструментів можуть виникнути такі аварійні ситуації
 - 1) Коротке замикання ланцюга живлення електроінструменту і загоряння електричних кабелів;
 - 2) Приховані електричні кабелі можуть бути пошкоджені та закорочені, що призведе до пожежі;
 - 3) Пошкодження прихованих трубопроводів, з яких можуть виділятися небезпечні рідини, пари або гази; і
 - 4) Ураження електричним струмом
 - 5) Вплив небезпечних рідин, парів і газів;
 - 6) Інші аварійні ситуації, не пов'язані безпосередньо з роботою електроінструменту.

Висновки

У даному дипломному проєкті побудовано та реалізовано охоронну систему стаціонарно віддаленого об'єкту підвищеної захищеності, так як у сучасному світі збільшується кількість та складність загроз які вимагають постійного вдосконалення заходів безпеки.

В ході вибору охоронних приладів для блокування об'єкту було віддано перевагу вітчизняним виробникам (Аjah) так як їхня якість відповідає європейським стандартам якості та технічним вимогам.

Оволодів загальними відомостями про охоронні системи, ознайомився з сучасними технологіями та принципом роботи в охоронних системах. Побудував ефективну охоронну систему для об'єкта підвищеної захищеності, з використанням охоронних приладів, систем відеонагляду та системи контролю доступу.

Одержав навички як правильно монтувати прилади охоронної системи дотримуючись рекомендацій з охорони праці. Опанував гідні навички у налаштуванні охоронної системи та максимально викоренив всі небезпечні та вразливі місця на об'єкті за допомогою охоронної сигналізації.

Зразок побудованої охоронної системи здатна виявляти та реагувати на потенційні загрози в режимі реального часу, забезпечуючи реагування органів влади, а також прогнозувати дії у сфері безпеки на віддалених територіях. Зокрема, охоронна система, яка наведена в дипломному проєкті, використовує передові технології і відповідає сучасним стандартам безпеки. Завдяки побудованій охоронній системі, кожен кабінет максимально захищений з мінімальними сліпими зонами.

Перелік умовних позначень

ППК – прилад приймально-контрольний
ОС – охоронна сигналізація
ОПС – охоронно пожежна сигналізація
ПЦС – пульт централізованого спостереження
СКД – система контролю доступу
ПЗ – програмне забезпечення
СТС – система тривожного сповіщення
ЕОМ – електро обчислювальна машина
ЗІЗ – засоби індивідуального захисту
GSM – Global System for Mobile (стандарт цифрового мобільного зв'язку)
GPRS – General Packet Radio Service (стандарт який використовує не зайняту смугу частот для передачі інформації)

Список використаних джерел

1. <https://ajax.systems.ua/blog/cyber-safety-essentials/>
2. https://www.bezpeka-shop.com/ua/catalog/tsentrali_i_pulty/
3. <https://vbezpeka.com.ua/uk/product/prilad-prijmalno-kontrolnij-ohoronno-pozhezhnij-lun-19/>
4. <https://shpalerkley.cx.ua/473-pristrij-ohoronnih-sistem-dlja-privatnogo-budinku.html>
5. <https://prel.prom.ua/g24866254-ohoronni-sistemi-signalizatsiyi>
6. <https://bezpeka.club/ohoronna-systema-z-chogo-vona-skladayetsya-i-yak-funktsionuye>
7. <https://worldvision.com.ua/ajax-hub-plus-white>
8. <https://worldvision.com.ua/ppk-orion-nova-m>
9. <https://worldvision.com.ua/ajax-keypad-plus-white>
10. <https://s-p.zone/wp-content/uploads/DSTU-4030-2001.pdf>
11. <https://ajax.systems.ua/blog/ajax-devices-certified-incert/>
12. http://ufib.com.ua/images/stories/50131_2_4.pdf
13. http://ufib.com.ua/images/stories/50131_2_4.pdf
14. https://el-sys.com.ua/solution_5
15. <https://klaster.ua/ua/stati-i-obzory/ohranno-pozharnaya-signalizaciya/>
16. <https://klaster.ua/ua/stati-i-obzory/ohranno-pozharnaya-signalizaciya/>
17. <https://pipl.ua/article/ohoronna-signalizaciya-lun-oglyad-rishen>
18. <https://alarm.lviv.ua/systemy-bezpeky/okhoronni-systemy/systemy-okhorony-dlia-bahatokvartyrnykh-budynkiv>
19. <https://crow.ua/>