

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи безпеки
приватного домоволодіння»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Юрій Костюк

Керівник професор кафедри КІ та КБ, д. т. н., доцент

 Володимир Воротнік

Рецензент доцент кафедри КІ та КБ, к. т. н., доцент

 Володимир Котенко

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Костюк Юрій Валерійович

Тема роботи: «Проект системи безпеки приватного домоволодіння»

затверджена Наказом університету від 1 березня 2023 р. №99/с

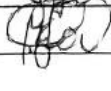
Термін здачі студентом закінченої роботи 10 червня 2023р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Предметом дослідження є використання програмованих контролерів в організації системи безпеки приватного домоволодіння, а об'єктом дослідження – процес побудови системи захисту приватного дооволодіння.

Обладнання та програмне забезпечення:

1. Пристрої та датчики фірми Ajax.
2. Відеореєстратор та відеокамери Hikvision.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В.В.		
2	Єфіменко А. А.		
3			

Студент  Юрій Костюк

Керівник  Володимир Воротніков

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023	
2	Аналіз існуючих рішень систем безпеки приватних домоволодінь	02.03 – 16.03.2023	
3	Розробка структури системи	17.03 – 17.04.2023	
4	Підбір компонентів для реалізації розробленої системи	26.04 – 02.05.2023	
5	Розробка програмного забезпечення для мікроконтролерів	03.05 – 03.06.2023	
6	Тестування розробленої системи	04.06 – 11.06.2023	
7	Оформлення пояснювальної записки	12.06 – 22.06.2023	
8	Захист дипломної роботи		

Студент  Юрій Костюк

Керівник  Володимир Воротніков

АНОТАЦІЯ

Текстова частина викладена на 60 сторінках друкованого тексту. Пояснювальна записка має 14 сторінок додатків. Список використаних джерел містить 20 найменувань та займає 2 сторінки. В роботі наведено 26 рисунків. Загальний обсяг роботи – 74 сторінки.

Мета кваліфікаційної роботи полягає у розробці системи безпеки приватного домоволодіння

У кваліфікаційній роботі досліджено та налаштовано апаратні засоби та розроблено програмне забезпечення, яке використовується для функціонування системи пожежної безпеки. Розглянуто особливості побудови таких систем та проаналізовано їх переваги та недоліки.

Проведено проектування системи, наведено схеми її роботи та взаємодії пристроїв в ній.

Після розробки проекту системи наведено процес її налаштування та тестування.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, AJAX, WIFI, HIKVISION, ДАТЧИК, ХАБ, СИСТЕМА БЕЗПЕКИ.

					КІК.КР.Б – 125 – 09 – ПЗ				
Зам.	Арк.	№ докум.	Підпис	Дата	Проект системи безпеки приватного домоволодіння	Літ.	Арк.	Аркушів	
Рспроб.		Костик Ю.В.		20.06.23					
Керівник		Воробієв В.В.		20.06.23			4	44	
Рспецп.		Комітетов В.М.		20.06.23		ФІКТ, Гр. КБ-19-1			
Н. контр.		Воробієв В.В.		20.06.23					
Затверд.		Сфіденко А.А.		20.06.23					

ANNOTATION

The textual part is presented on 60 pages of the printed text. The explanatory note consists of 14 pages of appendices. The list of references includes 20 items and occupies 2 pages. The work includes 26 figures. The total volume of the work is 74 pages.

The aim of the qualification work is to develop a security system for a private residential property.

The qualification work investigates and configures the hardware components and develops software used for the operation of the fire safety system. The construction features of such systems are considered and their advantages and disadvantages are analyzed.

The design of the system is conducted, including the schematics of its operation and device interaction.

After the development of the system project, the process of its configuration and testing is described.

Keywords: INTERNET OF THINGS, AJAX, WIFI, HIKVISION, SENSOR, HUB, SECURITY SYSTEM.

		Костюк Ю. В.			<i>КІК.КР.Б - 125 - 09 - 173</i>	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП	8
Розділ 1. Теоретичні аспекти побудови систем безпеки домоволодінь	9
1.1 Загальні принципи побудови систем безпеки домоволодінь.....	9
1.2 Принципи побудови охоронних систем та систем відеоспостереження ...	17
1.3 Принципи побудови систем протипожежної безпеки	20
1.4 Принципи захисту системи безпеки	21
1.5 Висновки з розділу 1	24
Розділ 2. Проектування системи безпеки приватного домоволодіння.....	25
2.1 Розробка загального проєкту системи безпеки приватного домоволодіння	25
2.2 Проектування охоронної підсистеми.....	29
2.3 Проектування підсистеми відеоспостереження	31
2.4 Проектування підсистеми пожежної безпеки.....	32
2.5 Висновки з розділу 2	34
Розділ 3. Практична реалізація системи безпеки приватного домоволодіння ...	35
3.1 Вибір обладнання та засобів реалізації проєкту системи безпеки приватного домоволодіння.....	35
3.2 Встановлення та налагодження підсистем та їх елементів	51
3.3 Тестування функціоналу окремих підсистем та системи в цілому	55
3.4 Висновки з розділу 3	56
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	58
ДОДАТКИ.....	60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT - Internet of Things.

Wi-Fi - Wireless Fidelity.

HD – High Definition.

CMOS - Complementary Metal-Oxide-Semiconductor.

CVBS - Composite Video Blanking and Sync.

GSM - Global System for Mobile.

		Костюк Ю. В.			<i>КІК.КР.Б - 125 - 09 - ПЗ</i>	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. Системи безпеки приватного домоволодіння мають велику актуальність у сучасному світі, де зростає кількість злочинів, пов'язаних зі зламами, крадіжками та вторгненнями. Захист особистих майнових цінностей і безпеки мешканців є надзвичайно важливим завданням, і розробка проекту системи безпеки приватного будинку стає необхідністю.

Однією з ключових причин для розробки такої системи є зростання кількості технологій, доступних як для зловмисників, так і для власників будинків. Зловмисники все більше використовують розумні технології та інтернет-підключення для викрадення даних, вторгнень або крадіжок. Тому власники будинків повинні бути в курсі останніх тенденцій у сфері систем безпеки та застосовувати передові технології для захисту свого житла.

Метою кваліфікаційної роботи є розробка системи безпеки приватного домоволодіння.

Для досягнення поставленої мети необхідно виконати наступні задачі:

- *проаналізувати існуючі підходи до створення систем безпеки;*
- *створити структуру системи безпеки, що складається з підсистем;*
- *розробити систему безпеки приватного домоволодіння.*

Об'єктом дослідження є процес побудови системи безпеки приватного домоволодіння.

Предметом дослідження є використання пристроїв IoT в організації системи безпеки приватного домоволодіння.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ СИСТЕМ БЕЗПЕКИ ДОМОВОЛОДІНЬ

1.1 Загальні принципи побудови систем безпеки домоволодінь

Система безпеки домоволодінь - це комплексний набір заходів, пристроїв і технологій, спрямованих на забезпечення безпеки мешканців та майна в приватних житлових приміщеннях. Вона включає в себе різноманітні системи, такі як системи відеоспостереження, контролю доступу, сигналізації, датчики пожежі, датчики руху та інші, які працюють разом для виявлення потенційних загроз та реагування на них.

Основне призначення систем безпеки домоволодінь - це захист жителів і майна від небезпек, таких як крадіжки, пожежі, несанкціоноване проникнення та інші небажані події. Вони допомагають виявляти небезпеку в ранній стадії, забезпечують швидку реакцію і допомогу, та можуть запобігти подальшим негативним наслідкам.

Системи безпеки домоволодінь можуть бути складними інтегрованими системами з централізованим управлінням або простими автономними пристроями. Вони можуть містити такі компоненти, як камери відеоспостереження, датчики руху, детектори диму та вогню, сирени, системи контролю доступу та інші.

Визначення систем безпеки домоволодінь включає в себе ідентифікацію потенційних загроз, оцінку ризиків, вибір і встановлення відповідних пристроїв та технологій, проектування системи, інтеграцію компонентів, налаштування та тестування системи, а також навчання мешканців щодо користування нею та процедур безпеки.

Враховуючи унікальні потреби та вимоги кожного будинку, система безпеки може бути налаштована для надання максимального рівня безпеки та спокою мешканцям.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Забезпечення безпеки в житлових приміщеннях має велику важливість і є однією з основних пріоритетів для будь-якої людини. Ось кілька ключових аспектів, які підкреслюють важливість безпеки в житлових приміщеннях:

1. Захист життя та здоров'я: Безпека в житлових приміщеннях прямо пов'язана з захистом життя та здоров'я мешканців. Наявність систем безпеки, таких як пожежна сигналізація, датчики витоку газу або системи відеоспостереження, допомагає виявляти небезпеку і реагувати на неї швидко і ефективно, що може запобігти травмам, втратам майна або навіть врятувати життя.

2. Запобігання крадіжкам та злочину: Системи безпеки, такі як сигналізаційні системи та системи контролю доступу, допомагають запобігти крадіжкам та злочину. Присутність видимої системи безпеки може відлякувати потенційних злочинців, а звукові та візуальні сигнали можуть сповістити про незаконне проникнення та привернути увагу оточуючих або служб безпеки.

3. Попередження пожеж: Датчики диму та системи пожежної сигналізації є невід'ємною частиною систем безпеки в житлових приміщеннях. Вони спроможні виявити пожежу у ранній стадії і сповістити мешканців про неї, дозволяючи їм вчасно евакуюватись та викликати пожежну службу для припинення поширення вогню та мінімізації збитків.

4. Спокій та психологічний комфорт: Безпека в домі створює спокій та психологічний комфорт для мешканців. Знання про те, що їхні житлові приміщення захищені від небезпеки, дозволяє людям відчувати себе безпечно і розслаблено у власному середовищі.

5. Захист майна: Системи безпеки також допомагають захистити майно від крадіжок та злочину. Сигналізаційні системи, системи відеоспостереження та інші пристрої забезпечують постійний нагляд і можуть попередити про незаконні вторгнення або небажану активність, що дозволяє своєчасно прийняти заходи для захисту майна.

Узагальнюючи, забезпечення безпеки в житлових приміщеннях є необхідною умовою для створення комфортного, безпечного та захищеного

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

середовища для мешканців. Ефективні системи безпеки забезпечують раннє виявлення небезпек, оперативну реакцію на них та запобігають можливим негативним наслідкам.

Оцінка загроз та ризиків є одним з ключових принципів побудови систем безпеки домоволодінь. Цей принцип передбачає ідентифікацію потенційних загроз та визначення ризиків, пов'язаних з безпекою, з метою прийняття відповідних заходів для їх запобігання або зменшення. Вона включає такі етапи:

1. Ідентифікація загроз: Спеціалісти з безпеки проводять аналіз потенційних загроз, які можуть вплинути на безпеку житлових приміщень. Це можуть бути загрози, такі як крадіжки, зломи, пожежі, витoki газу, повені, стихійні лиха та інші небезпечні ситуації.

2. Оцінка ризиків: Після ідентифікації загроз проводиться оцінка ризиків, пов'язаних з цими загрозами. Ризик оцінюється на основі ймовірності виникнення загрози та можливих наслідків для безпеки мешканців та майна.

3. Класифікація ризиків: Оцінені ризики класифікуються за їхньою важливістю та пріоритетністю. Ризики, які можуть призвести до серйозних наслідків, визначаються як високі пріоритети і потребують негайного усунення або зменшення.

4. Розробка заходів мінімізації ризиків: На основі оцінки загроз і ризиків розробляються конкретні заходи для мінімізації ризиків. Це може включати встановлення систем безпеки, які дозволяють виявляти загрози та реагувати на них, застосування протипожежних заходів, встановлення систем контролю доступу та інших заходів безпеки.

5. Постійна оцінка та аналіз: Системи безпеки домоволодінь потребують постійного моніторингу та оцінки для виявлення нових загроз та зміни у ризиках. Це дозволяє адаптувати системи безпеки до змінних умов і забезпечити ефективну захисту.

Оцінка загроз та ризиків є критичним етапом у побудові систем безпеки домоволодінь, оскільки вона допомагає ідентифікувати потенційні небезпеки і вжити відповідних заходів для їх запобігання. Цей принцип дозволяє мешканцям

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

житлових приміщень відчувати себе безпечно і спокійно, знаючи, що їхні домівки захищені від можливих загроз.

Основні елементи системи безпеки домоволодінь включають:

Системи виявлення і сповіщення про пожежу: Ці системи включають детектори диму, детектори вогню та системи оповіщення, такі як димові сигналізатори, пожежні сповіщувачі та автоматичні сповіщувачі пожежної служби. Вони виявляють наявність пожежі та сповіщають мешканців про небезпеку.

Системи охоронної сигналізації: Ці системи включають датчики руху, датчики відкриття дверей та вікон, контроль доступу та системи сповіщення про вторгнення. Вони захищають домоволодіння від незаконного вторгнення та сповіщають про можливі порушення безпеки.

Системи відеоспостереження: Ці системи включають камери спостереження, відеореєстратори та монітори. Вони дозволяють відстежувати події, що відбуваються в приміщенні або навколо нього, та забезпечують візуальний контроль над безпекою.

Системи контролю доступу: Ці системи включають електронні замки, картки доступу, біометричні ідентифікатори та кодові клавіатури. Вони обмежують доступ до приміщень та забезпечують контроль над тим, хто має право входу.

Системи контролю повітря: Ці системи включають детектори викидів газу, вуглекислого газу та інших небезпечних речовин, а також системи вентиляції та кондиціонування повітря. Вони виявляють небезпеку отруєння або вибуху та забезпечують безпечні умови для життя.

Системи контролю води: Ці системи включають датчики протікання води, системи автоматичного відключення водопостачання та системи контролю якості води. Вони допомагають запобігти витокам води та можливному затопленню, а також забезпечують безпеку використання води.

Електронні системи керування освітленням та енергозбереження: Ці системи включають автоматизовані системи керування освітленням, вимикачі

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

затримки, датчики руху та системи управління споживанням електроенергії. Вони забезпечують ефективне використання енергії та забезпечують комфортне освітлення в приміщенні.

Інтеграція та управління є важливими принципами побудови систем безпеки домоволодінь. Ці принципи дозволяють об'єднати різні компоненти системи безпеки в єдину інтегровану систему, а також забезпечувати ефективне та зручне управління цією системою.

Однією з ключових складових інтеграції є зв'язок між різними елементами системи безпеки. Наприклад, система охоронної сигналізації може бути інтегрована з системою відеоспостереження, що дозволяє автоматично записувати відео при спрацюванні сигналізації. Також можуть бути налаштовані автоматичні реакції на певні події, наприклад, при спрацюванні датчика руху може автоматично відбуватись активація підсвітки та запис відео.

Управління системою безпеки домоволодінь зазвичай здійснюється через централізований пульт або мобільний додаток. Це дає можливість мешканцям зручно контролювати різні аспекти безпеки, такі як активація або деактивація системи охоронної сигналізації, перегляд відеозаписів з камер спостереження, керування освітленням та температурою, а також отримання сповіщень про події.

Додатковою можливістю є інтеграція системи безпеки з іншими "розумними" пристроями та системами в домоволодінні, наприклад, з системою "розумний дім". Це дозволяє автоматизувати різні процеси та забезпечити взаємодію між системами. Наприклад, при спрацюванні датчика диму може автоматично відбуватись відключення електрики та вентиляції, а також надсилатись сповіщення власнику про можливу пожежу.

Інтеграція та управління є важливими принципами, оскільки вони сприяють покращенню ефективності та зручності використання системи безпеки домоволодінь. Вони дозволяють забезпечити цілісність та взаємодію різних компонентів, а також забезпечують зручний доступ та управління для користувачів.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Автоматизовані реакції є важливим принципом побудови систем безпеки домоволодінь. Цей принцип передбачає налаштування системи безпеки таким чином, щоб вона могла автоматично реагувати на певні події або ситуації без втручання користувача.

Одним з прикладів автоматизованих реакцій є реагування на тривогу або виявлення небажаних подій. Наприклад, при спрацюванні датчика руху або датчика відкриття вікна, система безпеки може автоматично активувати сирену, відправити сповіщення власнику або навіть надіслати сигнал до місцевої охоронної служби. Такі автоматизовані реакції допомагають швидко виявляти потенційні загрози та приймати необхідні заходи без затримки.

Крім того, системи безпеки домоволодінь можуть мати автоматизовані реакції на небезпеку, наприклад, пожежу або витік води. При спрацюванні датчиків диму або води, система може автоматично вимикати електрику, відкривати вентиляційні отвори для видалення диму, або навіть активувати автоматичні системи гасіння пожежі. Це дозволяє мінімізувати пошкодження та забезпечити швидке реагування на небезпечні ситуації.

Крім автоматичних реакцій на загрози, системи безпеки домоволодінь можуть мати і автоматизовані реакції на підвищення комфорту або забезпечення енергоефективності. Наприклад, система може автоматично регулювати освітлення та температуру в залежності від часу доби, присутності людей або налаштованих пріоритетів. Це дозволяє ефективно використовувати ресурси та створює комфортні умови для мешканців.

Важливість автоматизованих реакцій полягає в тому, що вони забезпечують швидку та надійну реакцію на небезпеки, забезпечують зручність та ефективність управління системою безпеки домоволодінь та допомагають забезпечити комфортне та безпечне середовище для мешканців.

Резервне живлення є важливим принципом побудови систем безпеки домоволодінь. Цей принцип передбачає наявність альтернативного джерела живлення, яке забезпечує незалежну роботу системи безпеки у разі відключення основного електропостачання.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Резервне живлення гарантує безперебійну роботу системи безпеки навіть в умовах відсутності електроенергії, що може виникнути внаслідок аварій, природних лих або спрямованого відключення електропостачання. В таких ситуаціях, коли стандартні джерела живлення не працюють, резервне живлення забезпечує безперебійну роботу системи безпеки та збереження її функцій.

Резервне живлення може бути реалізоване за допомогою різних технологій, таких як батарейні системи, дизельні генератори, сонячні панелі або комбіновані рішення. Ці джерела живлення забезпечують постійний доступ до енергії та уникнення перерв у роботі системи безпеки.

Наявність резервного живлення дозволяє підтримувати функціонування системи безпеки домоволодінь протягом тривалого часу після відключення основного джерела живлення. Це важливо для забезпечення безпеки мешканців та збереження важливої інформації, отриманої системою безпеки.

Таким чином, резервне живлення є необхідним елементом систем безпеки домоволодінь, оскільки воно забезпечує незалежну роботу системи у разі відключення основного електропостачання, забезпечуючи безперебійну роботу та захист мешканців та майна.

Постійне оновлення та тестування є одним з важливих принципів побудови систем безпеки домоволодінь. Цей принцип передбачає постійне вдосконалення та оновлення системи безпеки для забезпечення її ефективності та надійності.

Оновлення системи безпеки включає в себе використання останніх технологій, програмного забезпечення та обладнання, які відповідають сучасним стандартам безпеки. Це означає, що система безпеки повинна бути здатною адаптуватися до нових викликів та загроз, які можуть виникати з часом. Наприклад, в умовах швидкого розвитку цифрових технологій, системи безпеки повинні вміти працювати з мережевими пристроями, хмарними рішеннями та іншими сучасними технологіями.

Тестування системи безпеки є необхідним етапом, щоб перевірити її функціональність, надійність та відповідність вимогам. Це включає проведення різних тестів, таких як тестування на проникнення, симуляцію аварійних

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

ситуацій, перевірку відповідності стандартам безпеки та інші види тестів, що дозволяють переконатися в правильному функціонуванні системи.

Постійне оновлення та тестування дозволяють виявляти потенційні проблеми, уразливості та дефекти у системі безпеки та вчасно їх усувати. Це забезпечує високий рівень безпеки та захисту домоволодінь, оскільки система завжди залишається актуальною та пристосованою до сучасних загроз.

Таким чином, постійне оновлення та тестування є важливими елементами побудови систем безпеки домоволодінь, оскільки вони забезпечують актуальність, ефективність та надійність системи у змінних умовах, а також дозволяють виявляти та усувати можливі проблеми з безпекою.

Важливість правильного планування та побудови систем безпеки домоволодінь важко переоцінити, оскільки це є фундаментальним етапом в процесі забезпечення безпеки та захисту в приватному житті. Правильне планування та побудова системи безпеки дозволяють ефективно виявляти, попереджувати та реагувати на потенційні загрози та небезпеки, забезпечуючи безпечне та захищене життя для мешканців.

Основна важливість правильного планування та побудови полягає в наступних аспектах:

1. Індивідуалізація та врахування потреб: Кожне домоволодіння має свої особливості, потреби та унікальні вимоги до системи безпеки. Правильне планування дозволяє враховувати ці особливості та створювати індивідуальні рішення, що відповідають конкретним потребам мешканців.

2. Визначення загроз та ризиків: Планування системи безпеки передбачає оцінку потенційних загроз та ризиків, які можуть стати загрозою для безпеки мешканців та майна. Це дозволяє виявити потенційні проблемні області та прийняти необхідні заходи для їх запобігання або мінімізації.

3. Вибір правильних технологій та обладнання: Планування системи безпеки включає вибір відповідних технологій, пристроїв та обладнання, які відповідають потребам та вимогам безпеки. Це можуть бути системи

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

відеоспостереження, протипожежні системи, системи контролю доступу, датчики руху та інші елементи безпеки.

4. Розташування та конфігурація: Правильне планування дозволяє визначити оптимальне розташування та конфігурацію елементів системи безпеки. Наприклад, розташування відеокамер, сенсорів руху та датчиків диму залежить від особливостей приміщення та можливих шляхів проникнення.

5. Інтеграція з іншими системами: Планування системи безпеки також включає інтеграцію з іншими системами, такими як системи освітлення, системи автоматизації будинку, системи управління енергоефективністю тощо. Це дозволяє створити комплексну та злагоджену систему, яка працює в єдності для забезпечення безпеки та комфорту.

6. Планування резервного живлення: Планування системи безпеки також передбачає резервне живлення для забезпечення неперервності роботи системи навіть під час вимкнення електроенергії. Це може включати використання акумуляторів, дизельних генераторів або сонячних батарей.

Враховання цих аспектів під час планування та побудови системи безпеки домоволодінь допомагає забезпечити ефективну та надійну захист мешканців та майна від потенційних загроз. Правильно спроектована система безпеки забезпечує спокій, комфорт та впевненість в безпеці у власному житлі.

1.2 Принципи побудови охоронних систем та систем відеоспостереження

Охоронні системи є комплексом технічних засобів, процедур і дій, спрямованих на забезпечення безпеки об'єктів, будівель, майна та людей. Їх основна мета полягає в запобіганні незаконним вторгненням, виявленні небажаних подій, тривоги та наданні швидкого реагування на випадки порушення безпеки.

Системи відеоспостереження є складовою частиною охоронних систем та використовуються для візуального контролю і спостереження за об'єктами. Вони включають в себе камери, системи запису та моніторингу, що дозволяють в

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

реальному часі або після події отримувати зображення та відео з визначених місць.

Безпека та захист стали важливими аспектами в сучасному світі з огляду на зростаючі загрози, злочинність, терористичні акти та інші ризики. Забезпечення безпеки має пріоритетне значення для захисту майна, життя та інтересів людей. Охоронні системи та системи відеоспостереження грають важливу роль у забезпеченні безпеки в різних сферах, включаючи:

- Житлові приміщення: Охоронні системи та системи відеоспостереження забезпечують захист житлових будинків, квартир та приватних осель від крадіжок, незаконного доступу та інших загроз. Вони створюють почуття безпеки та спокою у мешканців, а також допомагають у виявленні потенційних небезпек та тривог.

- Комерційні будівлі та підприємства: Безпека має велике значення для підприємств та комерційних об'єктів, оскільки вони зберігають велику кількість цінного майна, документів та інформації. Охоронні системи та системи відеоспостереження допомагають у запобіганні крадіжок, забезпечують контроль за доступом працівників, виявлення пожеж та інших аварійних ситуацій.

- Громадські місця: Безпека в громадських місцях, таких як торгові центри, аеропорти, стадіони та інші, є надзвичайно важливою. Охоронні системи та системи відеоспостереження допомагають у забезпеченні порядку, виявленні підозрілих дій, попередженні інцидентів та забезпеченні безпеки громадян.

Загалом, безпека та захист в сучасному світі є невід'ємною частиною нашого життя. Охоронні системи та системи відеоспостереження відіграють важливу роль у створенні безпечного середовища для проживання, роботи та відпочинку. Вони допомагають у запобіганні негативних подій, виявленні потенційних загроз та швидкому реагуванні на них, забезпечуючи захист майна, безпеку людей та спокій у суспільстві.

Побудова охоронних систем та систем відеоспостереження, які використовуються для забезпечення безпеки в різних приміщеннях, включаючи

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

будинки та офіси, базується на декількох принципах. Розглянемо детільніше кожен з них.

Перший принцип - аналіз та оцінка ризиків. Перед побудовою охоронної системи необхідно провести оцінку потенційних загроз та ризиків, що можуть виникнути. Це включає виявлення слабких місць, потенційних шляхів проникнення та ідентифікацію можливих небезпек. На основі цієї оцінки розробляється стратегія охорони та вибір відповідних технологій.

Другий принцип - використання сучасних технологій. Системи охорони та відеоспостереження базуються на різних технологіях, таких як камери відеоспостереження, датчики руху, контроль доступу, системи сигналізації тощо. Важливо вибрати надійні та передові технології, які забезпечать ефективне функціонування системи та виявлення потенційних загроз.

Третій принцип - розташування елементів системи. Розташування камер відеоспостереження, датчиків руху та інших елементів системи має бути обґрунтованим та продуманим. Важливо охопити всі ключові точки і зони, де можуть виникнути проблеми, такі як входи, вікна, цінні об'єкти тощо. Крім того, розташування елементів системи повинно бути таким, щоб уникнути зрушень та перешкод у їх роботі.

Четвертий принцип - інтеграція та зв'язок. Охоронні системи та системи відеоспостереження повинні бути інтегровані між собою, щоб забезпечити повноцінний захист. Це означає, що різні компоненти системи повинні працювати разом і обмінюватися інформацією. Наприклад, сигнал з датчика руху може активувати камеру відеоспостереження для запису події.

П'ятий принцип - автоматизовані реакції та відповідь. Сучасні охоронні системи мають можливість автоматично реагувати на певні події або загрози. Наприклад, вони можуть спрацьовувати автоматичну сигналізацію, повідомляти власника про небезпеку через мобільний додаток або надсилати сигнал до центральної служби безпеки. Це дозволяє швидко реагувати на ситуації та забезпечувати ефективну захист.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Останній принцип - постійне оновлення та тестування. Системи безпеки постійно розвиваються, тому важливо періодично оновлювати їх компоненти та програмне забезпечення. Також важливо регулярно проводити тестування системи, щоб переконатися у її працездатності та ефективності.

Побудова охоронних систем та систем відеоспостереження базується на декількох принципах, які включають аналіз ризиків, використання сучасних технологій, правильне розташування елементів системи, інтеграцію та зв'язок, автоматизовані реакції та постійне оновлення та тестування. Ці принципи допомагають забезпечити ефективну та надійну захисту житлових та комерційних приміщень, зменшуючи ризики злочинності та забезпечуючи спокій та безпеку власників.

1.3 Принципи побудови систем протипожежної безпеки

Принципи побудови систем протипожежної безпеки в приватних домоволодіннях є основою для забезпечення захисту від пожеж та максимального збереження життя та майна. Розглянемо детально кожен з принципів:

Перший принцип - аналіз ризиків. Для ефективної системи протипожежної безпеки важливо визначити потенційні загрози пожежі, що можуть виникнути в приватному домоволодінні. Це можуть бути електричні проблеми, використання вогню, погіршення вентиляції, наявність запальних матеріалів тощо. Аналіз ризиків допомагає ідентифікувати потенційні проблеми і розробити відповідні стратегії для їх усунення.

Другий принцип - використання вогнегасників та пожежних тривог. Установка вогнегасників у стратегічних місцях домоволодіння дозволяє швидко реагувати на невеликі загоряння та запобігати їх поширенню. Крім того, пожежні тривоги, які включають димові детектори та пожежні сигналізаційні системи, можуть вчасно сповістити мешканців про небезпеку та дати можливість евакуюватися.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Третій принцип - наявність протипожежного освітлення та виходів. Установка протипожежного освітлення, яке працює на аварійне живлення, дозволяє забезпечити достатнє освітлення під час пожежі, коли основне електропостачання може бути відключене. Також важливо мати належно означені виходи та евакуаційні шляхи, які будуть відомі всім мешканцям.

Четвертий принцип - сповіщення та співпраця з пожежним відділенням. Наявність домоволодіння в системі сповіщення пожежному відділенню та вчасне інформування їх про пожежу є дуже важливим. Це допомагає забезпечити швидку реакцію та прибуття пожежних бригад для гасіння пожежі.

П'ятий принцип - розробка плану евакуації та навчання. Кожному мешканцю домоволодіння варто знати план евакуації, який включає шляхи виходу, місце збору та контактну інформацію. Регулярне проведення навчань з пожежної безпеки допомагає усвідомити процедури евакуації та дії в небезпечних ситуаціях.

Кожен з цих принципів важливий для побудови ефективної системи протипожежної безпеки у приватному домоволодінні. Їх впровадження та виконання допомагають запобігти пожежам, забезпечити безпеку мешканців та зберегти майно в разі виникнення небезпеки.

1.4 Принципи захисту системи безпеки

Убезпечення системи безпеки приватного будинку від можливих видів атак є критично важливим для забезпечення безпеки мешканців та майна. Розглянемо детально деякі з найпоширеніших атак та принципи захисту від них:

1. Фізичний доступ:

Атаки, пов'язані з фізичним доступом, включають незаконне проникнення до будинку або доступ до фізичних компонентів системи безпеки. Для захисту від цих атак необхідно:

- Встановити міцні зовнішні двері та вікна, а також додаткові захисні пристрої, такі як решітки або протигази.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- Застосовувати фізичні бар'єри, такі як огорожі або паркан, для утруднення несанкціонованого доступу до будинку.

- Встановити систему контролю доступу, таку як електронні замки або системи розпізнавання відбитків пальців, для обмеження доступу лише авторизованим особам.

2. Відмова в обслуговуванні (DoS) атаки:

DoS-атаки спрямовані на перевантаження системи безпеки, що призводить до відмови в обслуговуванні. Для захисту від цих атак необхідно:

- Встановити систему захисту мережі, яка може виявляти та блокувати вразливість до DoS-атак.

- Використовувати брандмауери та інші захисні пристрої для контролю трафіку та фільтрації небезпечних пакетів даних.

- Застосовувати механізми обмеження швидкості або капчу для запобігання автоматизованому перевантаженню системи.

3. Вторгнення в мережу (проникнення):

Атаки на мережу спрямовані на незаконне проникнення до системи безпеки через мережеві з'єднання. Для захисту від цих атак необхідно:

- Встановити надійні паролі та логіни для мережевих пристроїв, включаючи маршрутизатори, IP-камери та системи керування.

- Використовувати захищені мережеві протоколи, такі як WPA2 для Wi-Fi з'єднань.

- Встановити фаєрволи та системи виявлення вторгнень для моніторингу та блокування небажаних мережевих активностей.

4. Компрометація даних:

Атаки на компрометацію даних спрямовані на незаконне отримання, зміну або видалення конфіденційної інформації. Для захисту від цих атак необхідно:

- Використовувати шифрування даних для захисту конфіденційної інформації під час її передачі та зберігання.

- Регулярно оновлювати програмне забезпечення, включаючи операційні системи, драйвери та програми безпеки, для виправлення відомих вразливостей.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

- Забезпечити фізичну безпеку зберігання даних, наприклад, захищені серверні кімнати або криптографічні сховища.

Ці принципи захисту допоможуть забезпечити надійну систему безпеки приватного будинку, знижуючи ризик можливих атак і зберігаючи безпеку мешканців та їх майна.

5. Соціальний інжиніринг:

Атаки соціального інжинірингу спираються на маніпуляцію людей для отримання несанкціонованого доступу до системи безпеки. Для захисту від цих атак необхідно:

- Підвищити освіченість щодо соціального інжинірингу серед мешканців будинку, наголошуючи на важливості не розголошувати конфіденційну інформацію та не передавати доступ до систем безпеки незнайомим особам.

- Використовувати сильні паролі та двофакторну аутентифікацію для ускладнення несанкціонованого доступу до системи.

6. Фішинг:

Фішингові атаки використовують підроблені електронні листи або веб-сторінки, щоб зловити особисті дані власника будинку. Для захисту від цих атак необхідно:

- Навчити мешканців будинку розпізнавати підозрілі електронні повідомлення та посилання, і бути пильними стосовно надання особистих даних через електронну пошту або веб-сторінки.

- Використовувати антивірусне програмне забезпечення та спам-фільтри, щоб виявляти та блокувати фішингові атаки.

7. Викрадення ідентичності:

Атаки на викрадення ідентичності стосуються отримання конфіденційної інформації для підробки особистості власника будинку. Для захисту від цих атак необхідно:

- Уважно контролювати особисту інформацію та обмежити доступ до неї, зокрема, не розголошувати особисті дані відкрито або на ненадійних веб-ресурсах.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Використовувати шифрування та захищені протоколи передачі даних для запобігання перехоплення та зловживання особистою інформацією.

Ці методи захисту допоможуть убезпечити систему безпеки приватного будинку від додаткових типів атак та зберегти безпеку мешканців та їх власності.

1.5 Висновки з розділу 1

В першому розділі було розглянуто основні принципи побудови систем безпеки, а також таких підсистем: охоронної, відеоспостереження та пожежної безпеки.

В процесі аналізу існуючих рішень та підходів до побудови систем безпеки було встановлено, що широко поширеним є використання центрального хаба як керуючого пристрою у технічних рішеннях різних виробників. Однак, також часто реалізуються системи без використання центрального хаба. У кожної з цих систем є свої переваги та недоліки, які були враховані під час проектування нашої системи безпеки.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2. ПРОЕКТУВАННЯ СИСТЕМИ БЕЗПЕКИ ПРИВАТНОГО ДОМОВОЛОДІННЯ

2.1 Розробка загального проєкту системи безпеки приватного домоволодіння

У сучасному світі безпека приватних будинків є одним із найважливіших аспектів для забезпечення спокою і комфорту власників. Для досягнення цієї мети використовуються комплексні системи безпеки, які включають охоронну підсистему, систему відеоспостереження та систему протипожежної безпеки. Ці підсистеми працюють взаємодіючи між собою для забезпечення максимального рівня безпеки та захисту.

Охоронна підсистема є основою системи безпеки будинку і відповідає за контроль доступу, виявлення вторгнень та тривожне оповіщення. Основною складовою охоронної підсистеми є сенсорні пристрої, такі як датчики відкриття дверей і вікон, детектори руху та скловибиття. Ці пристрої постійно моніторять стан периметру будинку і в разі виявлення незвичайних подій спрацьовує тривога, яка може бути перенаправлена на центральну станцію охорони або повідомлена власникам будинку через мобільний додаток або SMS-повідомлення.

Система відеоспостереження використовує камери, розташовані у стратегічних місцях навколо будинку, для відстеження подій та запису відео. Це дозволяє власникам будинку спостерігати за діями на подвір'ї, вхідними воротами або іншими областями ідентифікованого ризику. Записані відеоматеріали можуть використовуватися як докази в разі необхідності. Безпечний доступ до відеокамер може бути забезпечений за допомогою паролів, шифрування та інших заходів безпеки.

Система протипожежної безпеки включає димові датчики, теплові датчики та сповіщувачі пожежі, які забезпечують виявлення пожежі та вчасну реакцію на неї. Димові датчики спрацьовують при виявленні диму, що дозволяє вчасно попередити про можливу пожежу і запустити сигнал тривоги. Теплові датчики

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

виявляють підвищення температури, що може свідчити про виникнення пожежі, і також ініціюють тривогу. Система протипожежної безпеки також включатиме в себе автоматичне виключення електрики, спрінклерні системи та інші пристрої для активного гасіння пожежі.

Взаємодія між цими трьома підсистемами є надзвичайно важливою для забезпечення комплексного захисту будинку. Сенсори охоронної підсистеми можуть викликати сигнал тривоги в системі відеоспостереження, що дозволить власникам отримати візуальну інформацію про подію, а також записати її для подальшого аналізу. Крім того, в разі спрацювання системи протипожежної безпеки, якщо виявлено пожежу або дим, може викликатися тривога і запускатися система відеоспостереження для негайного візуального контролю ситуації та надання важливої інформації пожежним службам.

Загальна схема взаємодії між охоронною, системою відеоспостереження та системою протипожежної безпеки створює цілісний і надійний комплексний захист приватного будинку.

При виявленні будь-яких порушень безпеки або небезпечних ситуацій, система безпеки негайно реагує, активуючи відповідні заходи та повідомляючи власників про потенційну загрозу. Такий комплексний підхід забезпечує надійний захист приватного будинку, дозволяючи власникам мати повний контроль над безпекою свого майна та благополуччям родини. Загальна схема системи безпеки наведена на рисунку 2.1.

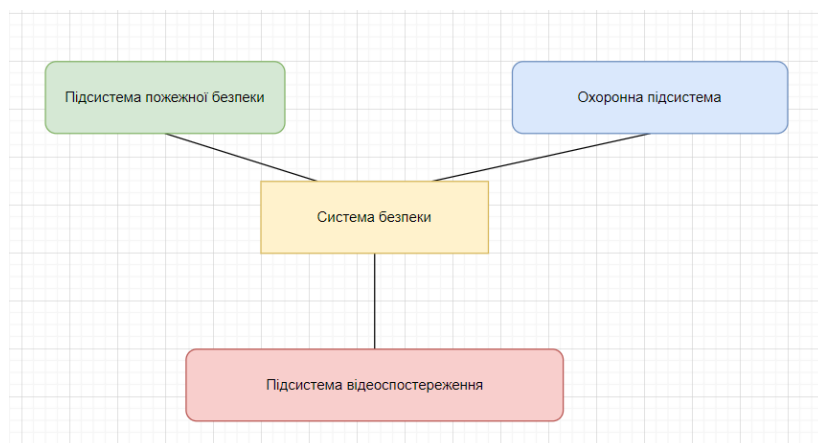


Рисунок 2.1 – Загальна схема системи безпеки

Розглянемо детальніше схему нашого приватного домоволодіння. Будинок знаходиться на території площею 298 квадратних метрів. Дана територія має один вхід(хвіртка) та один в'їзд(ворота) для автомобіля, будинок площею 204 квадратних метри(висота стін будинку 2.3 м) та 145 квадратних метрів дворової території. Загальна схема території наведена на рисунку 2.2.

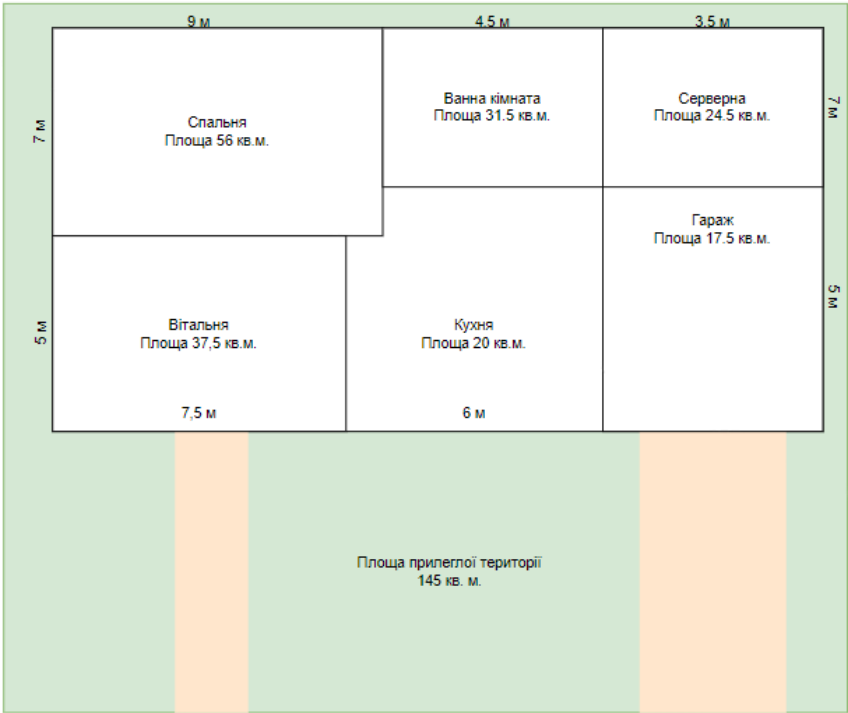


Рисунок 2.2 – Загальна схема території приватного домоволодіння

Будинок, схема якого наведена на рисунку 2.3, складається з 5 кімнат та гаража. В будинку 6 дверей, 6 вікон та одні гаражні ворота.

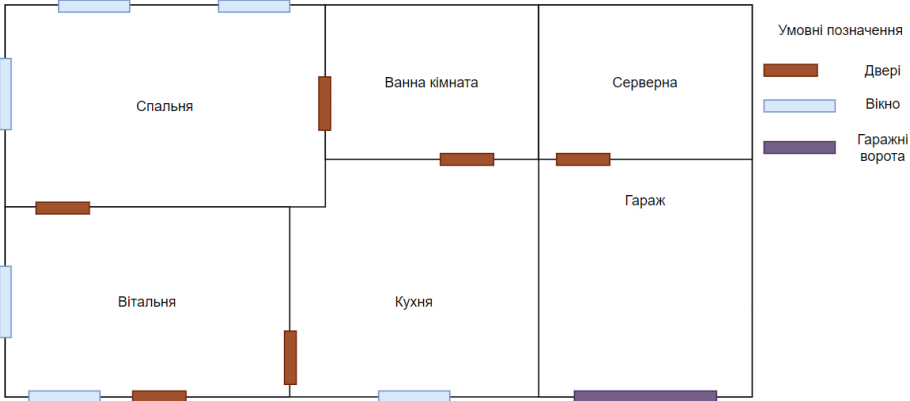


Рисунок 2.3 – Схема будинку

Система безпеки приватного будинку потребує надійного живлення для безперебійної роботи. У залежності від специфіки будинку та вимог власників, можуть використовуватись два основних типи живлення: основна система живлення та автономна система живлення з резервним джерелом.

Основна система живлення використовує електромережу будинку як основне джерело електроенергії для всіх компонентів системи безпеки. Це означає, що система безпеки буде працювати лише при наявності електричного живлення в будинку. У випадку відключення електроенергії через аварію, перебої в електромережі або навмисне відключення, основна система живлення може не забезпечити безперебійну роботу системи безпеки.

Тому важливим елементом системи безпеки є автономна система живлення з резервним джерелом. Ця система включає в себе батареї та генератори, які можуть забезпечити електроенергію в разі відключення основного джерела. Резервна система живлення буде автоматично включатись, коли виявиться відсутність електричного живлення в будинку, забезпечуючи безперебійну роботу системи безпеки протягом обмеженого часу.

Важливість наявності резервного живлення для системи безпеки важко переоцінити. Воно гарантує, що навіть при відключенні основного джерела електроенергії, система безпеки буде продовжувати працювати, забезпечуючи безпеку будинку та його мешканців. Це особливо важливо під час природних катастроф, стихійних лих або аварійних ситуацій, коли електромережа може бути пошкоджена або відключена на тривалий час. Наявність резервного живлення також забезпечує спокій власникам будинку, оскільки вони можуть бути впевнені, що система безпеки продовжує працювати навіть у випадку відсутності електропостачання. Це дозволяє вчасно виявляти потенційні загрози, викликати допомогу та забезпечувати безпеку житлового приміщення.

Отже, наявність резервного живлення є необхідною складовою частиною системи безпеки приватного будинку. Вона забезпечує безперебійну роботу системи навіть при відключенні основного джерела електроенергії і забезпечує постійний захист та безпеку будинку та його мешканців.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

2.2 Проектування охоронної підсистеми

Проектування охоронної підсистеми системи безпеки будинку включає кілька основних етапів, кожен з яких важливий для створення ефективної та надійної системи безпеки.

Перший етап - аналіз потреб і вимог - має вирішальне значення для успішного проектування системи безпеки будинку.

Для початку ідентифікуємо потенційні загрози. Такими можуть бути:

Вторгнення: Це одна з основних загроз, коли невинний чи небажаний особа намагається проникнути в будинок без дозволу. Вторгнення може бути здійснено шляхом фізичного проникнення через двері або вікна, використання підроблених ключів або незаконне використання кодів доступу до системи безпеки.

Вандалізм: Це малоцінне знищення або пошкодження власності. Вандали можуть намагатися пошкодити будівлю, автомобілі, садові нарізки або будь-які інші елементи майна. Це може призвести до фінансових збитків та порушення спокою мешканців.

Крадіжки: Крадіжки майна є серйозною загрозою для безпеки будинків. Це може включати крадіжки цінних речей, грошей, електроніки або інших цінних речей. Крадіжки можуть відбуватися під час відсутності мешканців або навіть під час їх присутності.

Незаконний доступ до будівлі: Це включає незаконне вторгнення до будинку через неправомірний доступ до системи контролю доступу або використання неправомірних методів для отримання доступу до будівлі.

Для уникнення потенційних загроз безпеці будинку в підсистемі мають бути такі компоненти як: датчики руху, датчики відкриття дверей та вікон, датчики розбиття скла, а також панель керування для активації та деактивації системи. Також потрібно використати електронні замки, картки доступу, біометричні системи (відбиток пальця, розпізнавання обличчя) або інші методи ідентифікації для контролю доступу до будинку.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Наступним етапом розробимо концептуальну схему системи безпеки, враховуючи вимоги наведені вище.

Керування пристроями підсистеми буде здійснюватись контролером(хабом), який буде розміщено у серверній. Підключення датчиків та систем контролю доступу здійснюватиметься за допомогою бездротового зв'язку через мережу Wi-Fi. Підсистема складатиметься з наступних датчиків:

руху в кожній кімнаті, а також надворі біля вхідних дверей та воріт гаража;
розбиття скла на кожному з вікон;

відкриття дверей на всіх дверях, вхідній хвіртці, воротах, а також на вікнах, що відкриваються;

Системи контролю доступу у вигляді сенсорних клавіатур буде розміщено на вхідних дверях та вході до серверної кімнати. Загальна схема розміщення пристроїв в будинку наведена на рисунку 2.4.

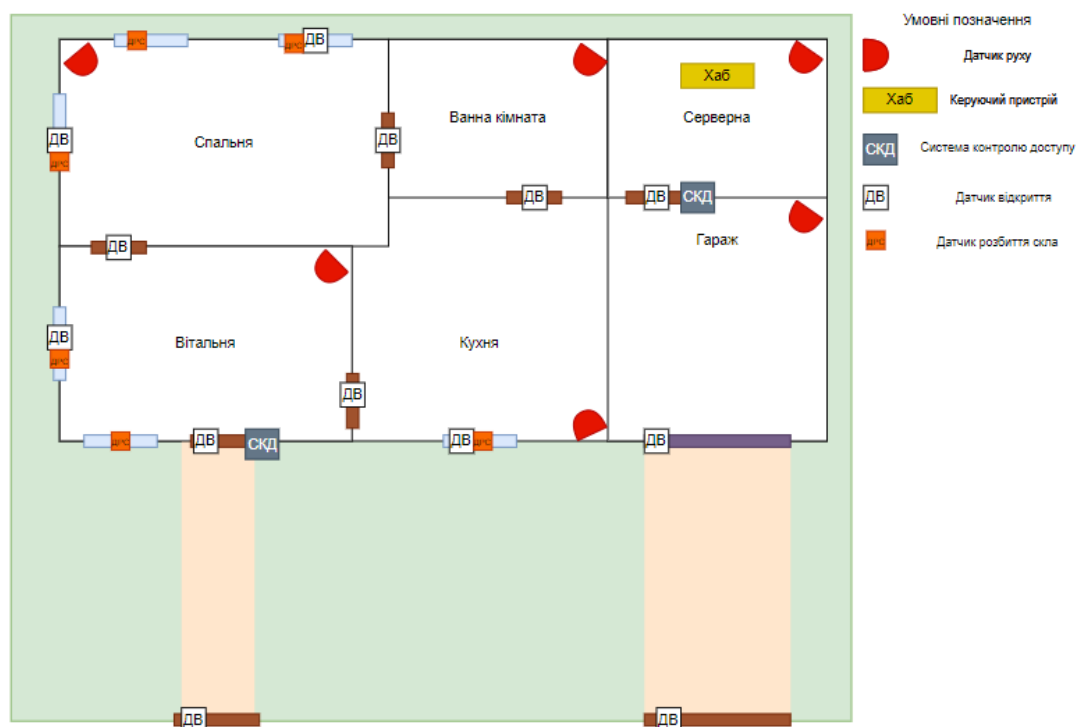


Рисунок 2.4 – Схема розміщення пристроїв охоронної підсистеми

2.3 Проектування підсистеми відеоспостереження

Системи відеоспостереження є ефективним та надійним засобом захисту від злочинців. Присутність відеокамер сама по собі є відлякувальним фактором для злочинців, а також може забезпечити докази в разі правопорушення на вашій власності. Успішна функціональність всієї системи відеоспостереження залежить від правильної установки камер.

Висота установки відеокамери визначає її поле зору та якість зображення. Камера, розташована біля входу в будинок або офісну будівлю, повинна мати широкий огляд, а також забезпечувати чітку видимість облич людей біля вхідних дверей. Наприклад, камера безпеки, встановлена на висоті 3 метрів, зможе фіксувати обличчя та розпізнавати типи статур людей. Рекомендується встановити одну камеру на висоті не менше 1 метра над вхідними дверима та іншу на висоті 3-6 метрів, спостерігаючи за транспортними засобами, що в'їжджають на подвір'я.

Невідповідне розташування камер відеоспостереження може призвести до незапису важливих кадрів. Важливо встановити камери відеоспостереження на всіх входах і в інших місцях, які потребують контролю.

Отже, правильно розташовані камери відеоспостереження є надійним і ефективним засобом захисту від загроз безпеці. Під час проектування підсистеми відеоспостереження важливо визначити об'єкти спостереження та зони охоплення камер. В нашому випадку об'єктами будуть:

периметр будинку;

входи та в'їзди на територію домоволодіння(як з внутрішньої так і з зовнішньої сторін);

кожна кімната будинку(окрім ванної кімнати) та гараж.

Під час проектування розміщення камер було враховано особливості розміщення об'єктів спостереження та використано мінімальну кількість відеокамер для спостереження за ними.

Керування камерами відеоспостереження, перегляд зображень із них та інші дії пов'язані зі спостереженням будуть виконуватись за допомогою

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

відеореєстратора, який буде розміщено у серверній кімнаті. Також у серверній кімнаті буде розміщено сховище даних, де зберігатимуться записи з камер. Схема розміщення пристроїв підсистеми відеоспостереження наведена на рисунку 2.5.

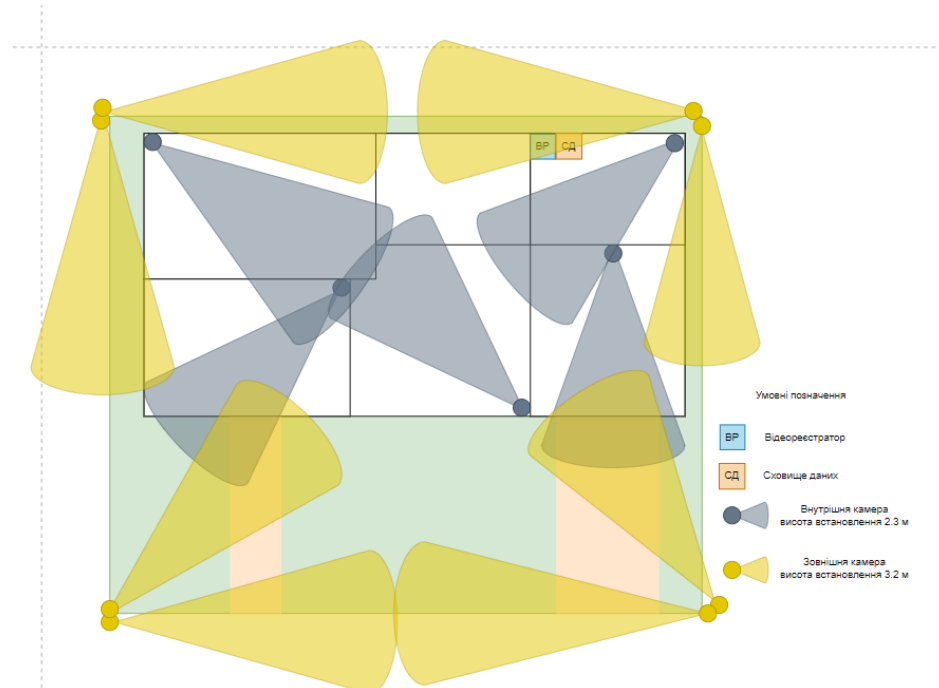


Рисунок 2.5 – Схема розміщення пристроїв підсистеми відеоспостереження

2.4 Проектування підсистеми пожежної безпеки

Проектування пожежної підсистеми системи безпеки будинку також включає кілька важливих етапів, починаючи з аналізу потреб і вимог. Під час аналізу необхідно визначити основні загрози пожежі та врахувати специфіку будинку і його розташування.

Наступним кроком є визначення необхідних компонентів пожежної підсистеми. Це можуть бути детектори диму, теплові датчики, система оповіщення про пожежу, пожежні тривожні кнопки та система автоматичного виклику пожежної служби. Детектори диму та теплові датчики реагують на зміни у рівні температури або наявність диму, спрацьовуючи тривогу у разі виявлення пожежі. Система оповіщення передає тривогу мешканцям будинку шляхом

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

активування звукових сигналів або візуальних сигналів, а також може включати систему автоматичного виклику пожежної служби для негайного реагування.

Після визначення компонентів необхідно розробити план розташування і розстановки детекторів та інших пристроїв. Це включає визначення оптимальних місць установки димових датчиків, теплових датчиків та пожежних тривожних кнопок. Важливо враховувати особливості будинку, такі як кількість поверхів, розташування спальних кімнат та виходів, щоб забезпечити належний охоплення пожежною підсистемою.

Отже, підсистема пожежної безпеки буде підключення до пристрою керування(хабу) та складатиметься з датчиків виявлення вогню та диму, спринклерів для автоматичного пожежогасіння, а також з силового реле, яке при виявленні пожежі знеструмлюватимуть будинок. Загалом для даної підсистеми необхідно 6 датчиків виявлення вогню та диму, 6 спринклерів та одне силове реле, а також 4 тривожні кнопки, які буде розміщено у всіх кімнатах, окрім серверної та ванної кімнати. Загальна схема підсистеми пожежної безпеки наведена на рисунку 2.6.

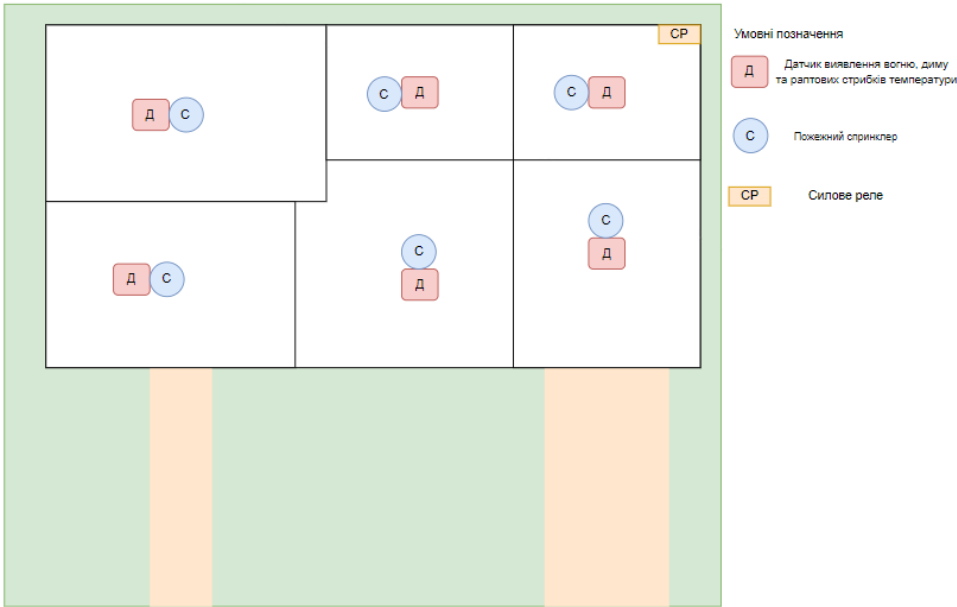


Рисунок 2.6 – Схема розміщення пристроїв підсистеми пожежної безпеки

2.5 Висновки з розділу 2

У другому розділі була розроблена система безпеки для приватного домоволодіння. Після аналізу різних підходів до побудови систем було вирішено використовувати комбінований підхід: деякі підсистеми працюватимуть без центрального хаба в якості керуючого пристрою, тоді як інші підсистеми будуть включати його в свою структуру.

Таке рішення дозволило нам розділити систему на різні підсистеми, деякі з яких будуть взаємодіяти між собою за допомогою центрального хаба. Кожна підсистема буде управлятися відповідними пристроями та хабом, що сприятиме рівномірному розподілу навантаження в системі.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ПРИВАТНОГО ДОМОВОЛОДІННЯ

3.1 Вибір обладнання та засобів реалізації проєкту системи безпеки приватного домоволодіння

Після того як систему та її підсистеми було спроектовано необхідно обрати засоби для забезпечення їх повного функціонування.

Оскільки підсистема відеоспостереження буде реалізовуватись без центрального хабу, розпочнемо вибір обладнання саме з неї.

Основним елементом керування та управління відеоспостереженням є відеореєстратор. Він повинен мати достатню кількість інтерфейсів для підключення всіх камер та достатню обчислювальну потужність для обробки даних з них. Гарним варіантом є HIKVISION TURBO HD DS-7316NUN1-K4, зображений на рисунку 3.1.



Рисунок 3.1 – Відеореєстратор HIKVISION TURBO HD DS-7316NUN1-K4

Його основними перевагами є:

- роздільна здатність запису 1080p;
- швидкість запису при роздільній здатності 1080p в 25 кадрів в секунду;
- підтримка кодеків H.265+/H.265/H.264+ та H.264;
- підтримка відеовиходів HDMI(4K), VGA, CVBS для виведення зображення на монітор;

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- підтримка 4 SATA інтерфейсів ємністю до 8 ТБ кожен(всього 32 ТБ);
- 2 мережні інтерфейси RJ-45 10/100/1000 Мбіт/с;
- інтерфейси 2 USB 2/0, 1 USB 3.0, RS-232 та RS-485.

Враховуючи технічні характеристики та переваги даного відеореєстратора можна зробити висновок, що він є ідеальним варіантом основи підсистеми відеоспостереження.

Наступним важливим елементом підсистеми є сховище даних, на яке буде здійснюватись резервне копіювання відеозаписів. Оскільки обраний відеореєстратор підтримує об'єм пам'яті до 32 ТБ, то сховище даних необхідно обирати відповідно теж на 32 ТБ. Хорошим варіантом буде система зберігання даних Synology 2BAY DS223 (DS223), зображена на рисунку 3.2.

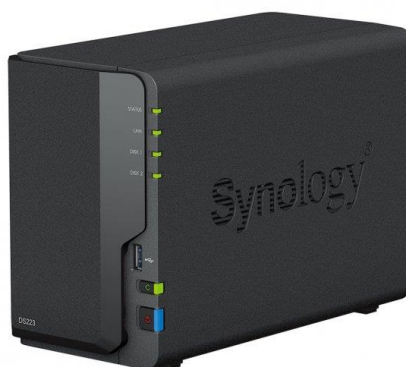


Рисунок 3.2 – Система зберігання даних Synology 2BAY DS223 (DS223)

Дане сховище даних підтримує віддалене та хмарне керування, що дозволить отримувати доступ до відеозаписів з будь-якої точки світу, 3 швидкісних інтерфейси USB 3.2 та високошвидкісну технологію GigabitEthernet, а також загальний об'єм накопичувачів до 32 ТБ, що є оптимальним для зберігання відеозаписів з камер спостереження. Отже, даний варіант сховища буде ідеальним для нашої підсистеми.

Наступним кроком перейдемо до вибору камер. В нашому варіанті підсистеми є 5 внутрішніх камер та 8 зовнішніх. Розташування камери є одним з важливих факторів при виборі оптимальної моделі.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Хорошим варіантом внутрішніх камер буде Hikvision DS-2CE56D0T-IRMMF(C) 3.6mm 2Мп Turbo HD, рисунок 3.3. Це купольна мультиформатна відеокамера з підтримкою стандартів HD-TVI, HD-CVI, AHD та CVBS. Вона оснащена 2Мп CMOS сенсором з чутливістю в кольорі 0.01 люкс та 0 люкс при увімкненій ІЧ-підсвітці дальністю до 20 м, роздільна здатність відео 1080р при частоті кадрів 25. Ця відеокамера призначена для організації внутрішнього відеоспостереження з використанням коаксіальних кабелів, а також модернізації вже існуючих систем. Доступна ціна, висока якість зображення, компактний дизайн та гнучкість інфраструктурних рішень роблять цю відеокамеру ідеальним вибором для систем відеоспостереження в приватних приміщеннях.



Рисунок 3.3 – Купольна відеокамера Hikvision DS-2CE56D0T-IRMMF(C)

Для організації зовнішнього відеоспостереження гарним варіантом буде камера Hikvision DS-2CE16D0T-IT5E 3.6mm 2Мп Turbo HD, рисунок 3.4. Це циліндрична Turbo HD камера з вбудованою ІЧ-підсвіткою серії EXIR 2.0 та підтримкою технології передачі живлення по PoC. Вона працює на базі світлочутливого сенсора 2 Мп CMOS з роздільною здатністю 1080р. Чутливість камери складає 0.01 люкс при апертурі 1.2, а при зйомці з увімкненою ІЧ-підсвіткою, яка освітлює відстань до 80 м – 0 Лк. Завдяки стандарту вологозахисту IP66 камера є ідеальним варіантом зовнішньої камери для спостереження за приватним домоволодінням.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		37



Рисунок 3.4 – Циліндрична камера Hikvision DS-2CE16D0T-IT5E

Вибір обладнання для підсистеми відеоспостереження завершено, перейдемо до вибору елементів охоронної підсистеми.

Оскільки пристрої підсистеми мають бути надійними, передавати дані захищеними каналами зв'язку та мати можливість управління з будь-якої точки світу, то вибір впав на обладнання компанії Ажах.

Ажах - це компанія, яка спеціалізується на виробництві та розробці інноваційних систем безпеки для домашнього використання, яка виробляє надійні та високоякісні системи безпеки, які включають в себе датчики руху, дверей/вікон, пожежу, вибух та інші функціональні компоненти. Ці системи працюють на основі передових технологій безпроводового зв'язку та забезпечують надійний моніторинг і захист приміщень. Компанія Ажах має широкий асортимент продуктів та надає зручне та інтуїтивно зрозуміле програмне забезпечення для керування системою. Вони також просунуті в галузі хмарних технологій, що дозволяє користувачам отримувати доступ до своєї системи з будь-якого місця за допомогою мобільного додатку. Завдяки своїм інноваціям та надійності, Ажах стала популярним вибором для домашньої безпеки у багатьох країнах, а отже підходить для реалізації нашої підсистеми.

У якості центрального керуючого пристрою буде використано центральний Hub 2 Plus, рисунок 3.4.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		38



Рисунок 3.4 – Централь Ajax Hub 2 Plus

Ajax Hub 2 Plus - це центральний хаб від компанії Ajax, призначений для управління системами безпеки в домашньому середовищі. Основні характеристики Ajax Hub 2 Plus включають в себе:

1. Багатофункціональність: Ajax Hub 2 Plus підтримує підключення до 200 пристроїв, таких як датчики руху, дверей/вікон, пожежні датчики та інші, що дозволяє широкий спектр захисту для приміщень.

2. Надійність: Ajax Hub 2 Plus працює на основі зв'язку з високою стабільністю, включаючи Ethernet, Wi-Fi та GSM, що забезпечує надійне з'єднання з серверами і забезпечує безперебійний моніторинг безпеки.

3. Захист від вторгнень: Ajax Hub 2 Plus оснащений системою захисту від вторгнень, включаючи захист від підмінення SIM-карти, захист від зламу та антиджемову технологію, що забезпечує високий рівень безпеки.

Переваги Ajax Hub 2 Plus:

- Простий монтаж та налаштування.
- Інтуїтивно зрозумілий і зручний інтерфейс для керування системою.
- Можливість підключення до хмарного сервісу для дистанційного керування та моніторингу.

Недоліки Ajax Hub 2 Plus:

- Висока ціна порівняно з іншими хабами на ринку.
- Потребує стабільного інтернет-з'єднання для оптимальної роботи.

Загалом, Ajax Hub 2 Plus є потужним та надійним центральним хабом для підсистеми безпеки та ідеальним варіантом для використання його в якості

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

основи нашої охоронної підсистеми. Після того, як керуючий пристрій обрано перейдемо до вибору датчиків.

Датчики руху мають покривати максимальну площу кімнати, бути надійними та захищеними від хибних спрацювань. Гарним варіантом такого датчика є Ajax MotionCam (PhOD), рисунок 3.5.



Рисунок 3.5 – Датчик руху з фотокамерою Ajax MotionCam(PhOD)

Ajax MotionCam (PhOD) - це бездротовий датчик руху від компанії Ajax з фотооптичним детектором. Цей датчик є частиною системи безпеки Ajax і використовується для виявлення руху в приміщеннях.

Основні характеристики та особливості Ajax MotionCam (PhOD):

1. Фотооптичний детектор: Він поєднує в собі руховий сенсор та фотокамеру, що дозволяє не тільки виявляти рух, але й отримувати зображення об'єкту, який спричинив спрацювання датчика. Це дозволяє отримати важливу інформацію про подію та швидко реагувати на неї.

2. Інтелектуальна обробка зображень: Ajax MotionCam (PhOD) використовує алгоритми комп'ютерного зору для виявлення людей на зображеннях. Це дозволяє зменшити кількість помилкових спрацювань, що можуть бути викликані рухом тварин або рухом рухливих предметів.

3. Висока надійність: Датчик Ajax MotionCam (PhOD) працює на основі бездротового протоколу Ajax, який забезпечує стабільне зв'язку між датчиком і центральним хабом. Він також має захист від перешкод та зламу.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

4. Додаткові функції: Датчик підтримує функції паніки та перевірки працездатності батареї. Він також має вбудований інфрачервоний освітлювач, що дозволяє робити якісні зображення навіть в умовах недостатнього освітлення.

Ajax MotionCam (PhOD) є інноваційним рішенням для систем безпеки Ajax, яке поєднує в собі виявлення руху та отримання зображень. Він дозволяє користувачам швидко реагувати на потенційні загрози та забезпечує високий рівень безпеки приміщень та прекрасно підходить для використання у нашій охоронній підсистемі.

Наступним кроком оберемо датчики відкриття вікон та дверей. Датчики відкриття дверей мають реагувати на відкриття в одному напрямку, на відміну від датчиків відкриття на вікнах, які мають опрацьовувати й відкриття з нахилом.

Для дверей використаємо датчики на базі геркона, а саме Ajax DoorProtect, рисунок 3.6.



Рисунок 3.6 – Датчик відкриття на базі геркона Ajax DoorProtect

Ajax DoorProtect - це бездротовий магнітний датчик, який призначений для захисту дверей та вікон у системі безпеки Ajax. Він використовується для виявлення відкриття або закриття дверей/вікон, що дозволяє ефективно контролювати доступ до приміщень.

Основні характеристики та особливості Ajax DoorProtect:

1. Магнітний датчик: Датчик складається з двох компонентів - головної одиниці та магнітного контакту. Коли двері або вікно відкриваються, розривається магнітне поле між цими компонентами, що призводить до спрацювання датчика.

2. Бездротовий протокол Ajax: Ajax DoorProtect працює на основі бездротового протоколу Ajax, що забезпечує надійний та шифрований зв'язок з

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

центральним хабом. Це забезпечує стабільну та безперебійну передачу сигналу з датчика до системи безпеки.

3. Довгий термін служби батареї: Датчик Ajax DoorProtect працює від батареї, яка має довгий термін служби. Це дозволяє використовувати датчик протягом тривалого часу без необхідності заміни батареї.

4. Простий монтаж та налаштування: Ajax DoorProtect легко встановлюється на двері або вікно за допомогою монтажних елементів, які входять в комплект. Його також легко налаштовувати та підключати до системи безпеки Ajax.

Ajax DoorProtect є надійним і ефективним датчиком для захисту дверей та вікон. Він допомагає підвищити рівень безпеки приміщень та швидко виявляти незаконне проникнення або небажані відкриття і буде чудовим варіантом для використання на дверях у нашій охоронній підсистемі.

На вікна ж буде встановлено датчик відчинення, удару та нахилу на базі геркона з акселерометром, а саме Ajax DoorProtect Plus, рисунок 3.7.



Рисунок 3.7 – Датчик Ajax DoorProtect Plus

Ajax DoorProtect Plus - це покращена версія бездротового магнітного датчика від компанії Ajax. Цей датчик призначений для захисту дверей та вікон у системі безпеки Ajax і має додаткові функції, які покращують його ефективність та надійність.

Основні характеристики та особливості Ajax DoorProtect Plus:

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

1. Двостороннє комунікування: Ajax DoorProtect Plus має здатність передавати не тільки інформацію про відкриття/закриття дверей або вікон, але й статус батареї та якість зв'язку. Це дозволяє оперативно виявляти проблеми та забезпечувати надійну роботу системи.

2. Довгий термін служби батареї: Датчик Ajax DoorProtect Plus має енергоефективну конструкцію, що забезпечує тривалий термін служби батареї. Це означає менше зусиль щодо заміни батареї та більш безперебійну роботу датчика.

3. Захист від підміни та зламу: Ajax DoorProtect Plus володіє захистом від підміни та зламу, що робить його стійким до спроб обходу системи. Він має вбудовану систему тривоги, яка спрацьовує при спробі несанкціонованого втручання.

4. Багатофункціональність: Ajax DoorProtect Plus може використовуватися не тільки для виявлення відкриття/закриття дверей та вікон, але і як панічна кнопка або для активації режиму "Домашня охорона". Це розширює його можливості та забезпечує більш гнучке використання.

Ajax DoorProtect Plus є надійним та функціональним датчиком, який забезпечує ефективний контроль за вікнами у системі безпеки Ajax. Він допомагає підвищити безпеку приміщень та швидко реагувати на будь-які небажані події або порушення.

Також на вікнах необхідно передбачити розбиття скла та встановити на них відповідні датчики. Ідеальним варіантом буде датчик розбиття скла Ajax GlassProtect, рисунок 3.8.



Рисунок 3.8 – Датчик розбиття скла Ajax GlassProtect

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Ajax GlassProtect - це бездротовий датчик, спеціально розроблений для виявлення розбиття скла у системі безпеки Ajax. Цей датчик використовується для захисту вікон, скляних дверей, вітрин та інших скляних поверхонь.

Основні характеристики та особливості Ajax GlassProtect:

1. Акустичне виявлення розбиття скла: Ajax GlassProtect використовує алгоритми акустичного виявлення, щоб спостерігати за звуковими характеристиками розбиття скла. Якщо виявляються характерні звуки, датчик спрацьовує та передає сигнал про подію до центральної системи безпеки.

2. Багатосторонній захист: Ajax GlassProtect виявляє розбиття скла з усіх сторін датчика, що робить його ефективним для використання на різних типах скляних поверхонь.

3. Бездротовий протокол Ajax: Датчик працює на бездротовому протоколі Ajax, що забезпечує надійний зв'язок з центральною системою безпеки. Це забезпечує швидку передачу сигналу та надійне сповіщення про розбиття скла.

4. Інтелектуальний аналіз звуку: Ajax GlassProtect використовує інтелектуальний аналіз звуку для відокремлення звуків розбиття скла від інших шумів у середовищі. Це зменшує вірогідність спрацювання датчика через помилкові сигнали.

5. Легкий монтаж та налаштування: Ajax GlassProtect легко встановлюється на скляну поверхню за допомогою спеціального клейкого шару або кріпильних елементів. Його також легко налаштовувати та підключати до центральної системи безпеки Ajax.

Отже, Ajax GlassProtect є надійним та ефективним датчиком для виявлення розбиття скла, що дозволяє підвищити безпеку приміщень та забезпечити швидку реакцію на небажані події.

Оскільки всі пристрої системи з'єднуються з керуючим пристроєм за допомогою бездротового зв'язку, то необхідно забезпечити високу якість сигналу для кожного з них. Для цього буде використано ретранслятор Ajax ReX 2, рисунок 3.9.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44



Рисунок 3.9 – Ретранслятор сигналу Ajax ReX 2

Ajax ReX 2 - це бездротовий ретранслятор сигналу, розроблений компанією Ajax Systems. Він використовується для розширення зони покриття бездротової системи безпеки Ajax, забезпечуючи стабільний зв'язок між датчиками та центральною системою.

Основні характеристики та особливості Ajax ReX 2:

1. Ретрансляція сигналу: Ajax ReX 2 отримує сигнали від бездротових пристроїв Ajax, таких як датчики руху, дверей, пожежні датчики тощо, і передає їх до центральної системи безпеки. Це дозволяє розширити зону покриття та забезпечити надійний зв'язок навіть у віддалених місцях.

2. Багатоканальність: Ajax ReX 2 підтримує одночасну роботу на кількох радіочастотних каналах, що забезпечує стійкий зв'язок та захист від перешкод.

3. Захист від перешкод та підміни: Ретранслятор Ajax ReX 2 володіє захистом від перешкод та спроб підміни. Він виявляє незвичайні радіосигнали та спрацьовує в разі виявлення спроб порушення безпеки.

4. Резервне живлення: Ajax ReX 2 оснащений вбудованим акумулятором, що дозволяє продовжити роботу ретранслятора при відсутності електроживлення. Це забезпечує безперебійну роботу системи навіть під час перебоїв електроенергії.

5. Легкий монтаж та налаштування: Ajax ReX 2 легко встановлюється та налаштовується за допомогою мобільного додатку Ajax. Його можна підключити до центральної системи безпеки Ajax шляхом бездротового зв'язку.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Ајах ReX 2 є надійним та ефективним ретранслятором, який розширює покриття бездротової системи безпеки Ајах та забезпечує стабільний зв'язок між пристроями та центральною системою.

В ролі системи контролю доступу для керування сигналізацією будинку буде використано охоронну клавіатуру Ајах KeyPad Plus, рисунок 3.10.



Рисунок 3.10 – Охоронна клавіатура Ајах KeyPad Plus

Ајах Keypad Plus - це охоронна клавіатура, розроблена компанією Ајах Systems, яка використовується для керування системою безпеки Ајах. Ця клавіатура надає зручний та простий спосіб керування безпековою системою і забезпечує додатковий рівень безпеки для об'єкту.

Основні характеристики та особливості Ајах Keypad Plus:

1. Зручне керування: Ајах Keypad Plus має кнопки зручного розташування, які дозволяють легко ввімкнути або вимкнути охоронний режим системи, а також активувати інші режими (наприклад, "домашній" режим)

2. Система введення PIN-коду: Клавіатура має вбудовану систему введення PIN-коду для автентифікації користувача. Це забезпечує безпеку та захист від несанкціонованого доступу до системи.

3. Статусна індикація: Ајах Keypad Plus відображає статус системи безпеки, що дозволяє користувачу швидко перевірити, чи активований охоронний режим, чи є тривоги, або чи є будь-які помилки.

4. Бездротове підключення: Клавіатура підключається до центральної системи безпеки Ајах за допомогою бездротового зв'язку, що дозволяє розміщати її в зручному для користувача місці.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

5. Індивідуальні налаштування: Ajax Keypad Plus може бути налаштована під потреби користувача. Вона підтримує налаштування різних режимів безпеки, програмування сповіщень та інші персоналізовані налаштування.

Ajax Keypad Plus є надійним і простим у використанні засобом керування безпековою системою Ajax, який доповнює функціональність системи та забезпечує зручну та безпечну роботу з нею.

Наступними підберемо елементи для підсистеми пожежної безпеки, які підключатимуться до хабу охоронної підсистеми. Основним елементом стане датчик тепла, диму та чадного газу зі змінними батареями Ajax FireProtect Plus, рисунок 3.11.



Рисунок 3.11 – Датчик тепла, диму та чадного газу зі змінними батареями Ajax FireProtect Plus

Ajax FireProtect Plus - це бездротовий датчик пожежі, розроблений компанією Ajax Systems. Він призначений для виявлення пожежі і передачі тривоги до центральної системи безпеки Ajax. Цей датчик забезпечує надійний моніторинг приміщень і реагує на підвищення температури та виникнення задимлення.

Основні характеристики та особливості Ajax FireProtect Plus:

1. Виявлення пожежі: Датчик Ajax FireProtect Plus виявляє підвищення температури та виникнення задимлення, що може свідчити про виникнення пожежі. Він миттєво спрацьовує та передає тривогу до центральної системи безпеки Ajax.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

2. Інтелектуальний алгоритм: Датчик використовує інтелектуальний алгоритм аналізу даних, що дозволяє точно виявляти пожежу та уникати неправдивих тривог.

3. Бездротовий зв'язок: Ajax FireProtect Plus працює на бездротовій технології, що дозволяє легко встановлювати його в будь-якому місці. Він підключається до центральної системи безпеки Ajax через захищений бездротовий протокол зв'язку.

4. Додаткові функції: Датчик може працювати в режимі температурного датчика, що дозволяє виявляти надмірне підвищення або зниження температури в приміщенні. Він також має вбудований звуковий сигналізатор для миттєвого виявлення пожежі.

5. Довгий термін служби батареї: Ajax FireProtect Plus має ефективну систему живлення, що дозволяє працювати довгий час без заміни батареї.

Ajax FireProtect Plus є надійним та ефективним датчиком пожежі, який забезпечує безпеку і швидку реакцію на виникнення пожежі в будь-якому приміщенні.

Наступним важливим елементом підсистеми пожежної безпеки є силове реле, яке здійснюватиме відімкнення будинку від електромережі у випадку пожежі. Ідеальним варіантом такого пристрою є силове реле Ajax WallSwitch, рисунок 3.12.



Рисунок 3.12 – Силове реле Ajax WallSwitch

Ajax WallSwitch - це силове реле, розроблене компанією Ajax Systems. Воно призначене для бездротового керування електричними навантаженнями в

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

системі безпеки Ajax. Ajax WallSwitch дозволяє включати та виключати електричні пристрої за допомогою центральної системи безпеки або мобільного додатку.

Основні характеристики та особливості Ajax WallSwitch:

1. Бездротове підключення: Силове реле Ajax WallSwitch підключається до центральної системи безпеки Ajax за допомогою бездротового зв'язку, що дозволяє легко управляти електричними навантаженнями з будь-якого місця.

2. Дистанційне керування: За допомогою мобільного додатку Ajax або пульта керування можна включати та виключати підключені до Ajax WallSwitch електричні пристрої зручною дистанційною кнопкою.

3. Режими роботи: Ajax WallSwitch підтримує різні режими роботи, такі як миттєве включення або виключення, таймери, планування, групове керування тощо. Це надає гнучкість та зручність в управлінні електричними пристроями.

4. Захист від перевантаження: Ajax WallSwitch має вбудований захист від перевантаження, що дозволяє уникнути пошкодження підключених пристроїв в разі надмірного навантаження.

5. Енергоефективність: Силове реле Ajax WallSwitch має низький споживання електроенергії, що дозволяє економити ресурси та забезпечує довгий термін роботи.

Ajax WallSwitch є зручним та надійним рішенням для бездротового керування електричними пристроями у системі безпеки Ajax, що додає зручність та автоматизацію в повсякденному використанні, а також дозволяє убезпечити будинок від короткого замикання під час пожежі.

Фінальним елементом нашої системи безпеки стануть автоматичні спринклери для пожежогасіння. Чудовим варіантом є спринклери швидкого реагування RAPIDROP RD021, рисунок 3.13.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49



Рисунок 3.13 – Спринклер швидкого реагування універсальний,
RAPIDROP RD021

Спринклер швидкого реагування універсальний RAPIDROP RD021 є пристроєм, призначеним для пожежного захисту приміщень. Він є частиною системи автоматичного пожежного гасіння, де реагує на виникнення підвищеної температури та активує струмінь води для пригнічення пожежі.

Основні характеристики та особливості спринклера RAPIDROP RD021:

1. Універсальний дизайн: RD021 є універсальним спринклером, що може використовуватися в різних типах приміщень, таких як офіси, магазини, склади, готелі тощо.

2. Швидка реакція: В разі підвищення температури спринклер RD021 активується швидко та автоматично. Він відкриває клапан та створює струмінь води, який допомагає пригнітити пожежу та запобігти її поширенню.

3. Простий монтаж: RD021 має простий монтажний процес. Він може бути легко встановлений на стелю або стіну приміщення згідно з вимогами пожежної безпеки.

4. Висока якість: Спринклер RD021 виготовлений з високоякісних матеріалів, що забезпечує його довговічність та надійність у роботі.

5. Ефективність: RD021 забезпечує ефективне гасіння пожежі, допомагаючи контролювати її розповсюдження та запобігати значним пошкодженням приміщення.

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

RAPIDROP RD021 є надійним та ефективним спринклером швидкого реагування, який допомагає забезпечити безпеку та захист від пожеж у різних типах будівель та приміщень.

На цьому вибір обладнання для нашої системи безпеки завершений.

3.2 Встановлення та налагодження підсистем та їх елементів

Перейдемо до встановлення та налагодження елементів підсистеми відеоспостереження. Розмістимо камери, відеореєстратор та сховище даних згідно з розробленою у розділі 2 схемою, з'єднаємо їх з відеореєстратором та встановимо накопичувачі. Для налаштування відеореєстратора завантажимо та встановимо програму SADP Tool, рисунок 3.14.

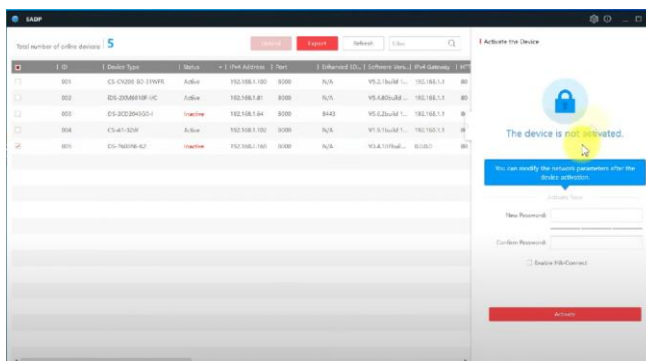


Рисунок 3.14 – Інтерфейс програми SADP Tool

Активуємо наш реєстратор та присвоюємо йому IP-адресу, рисунок 3.15.



Рисунок 3.15 – Присвоєння IP-адреси реєстратору

Після встановлення адреси переходимо до веб-інтерфейсу керування, рисунок 3.16, авторизуємось та завантажуюмо необхідний для роботи системи плагін.

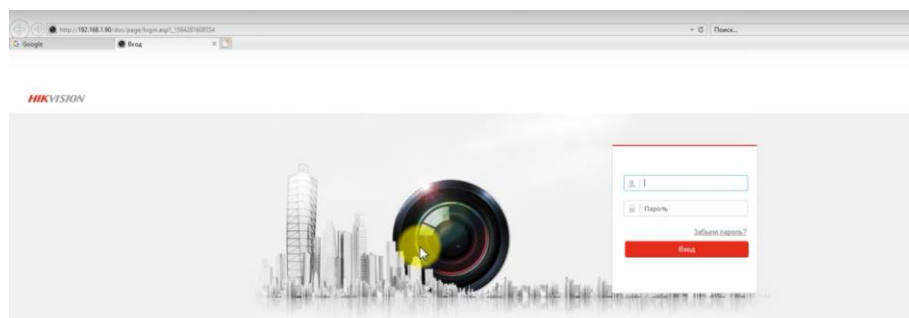


Рисунок 3.16 – Веб-інтерфейс керування відеореєстратором

В налаштуваннях встановлюємо синхронізацію часу з комп'ютером та переходимо до панелі додавання камер та натискаємо кнопку швидкого додавання, рисунок 3.17.

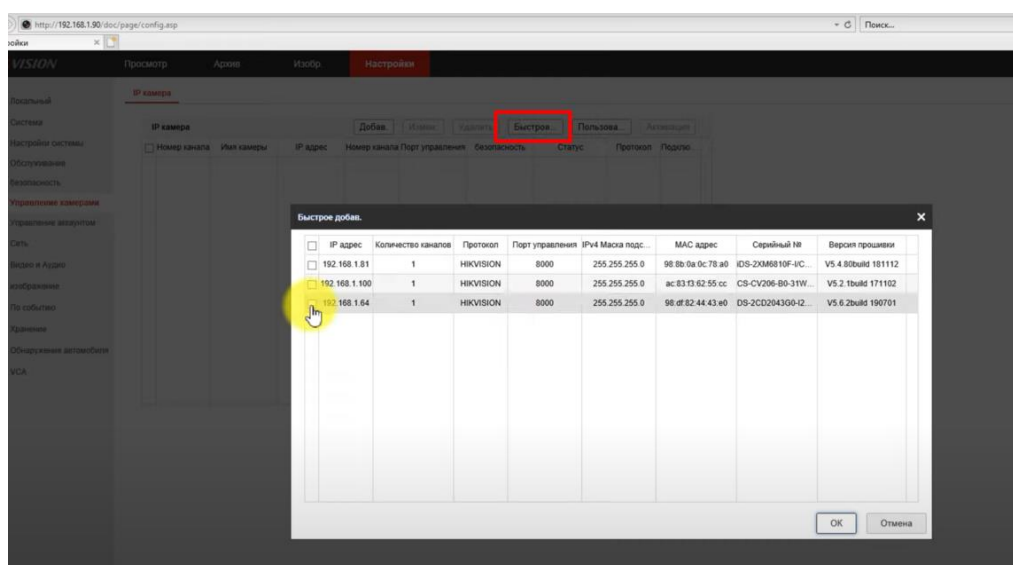


Рисунок 3.17 – Швидке додавання камери Hikvision

Додаємо обрану камеру та активуємо її за допомогою пароля адміністратора, рисунок 3.18, після чого камера з'явиться в мережі, рисунок 3.19.

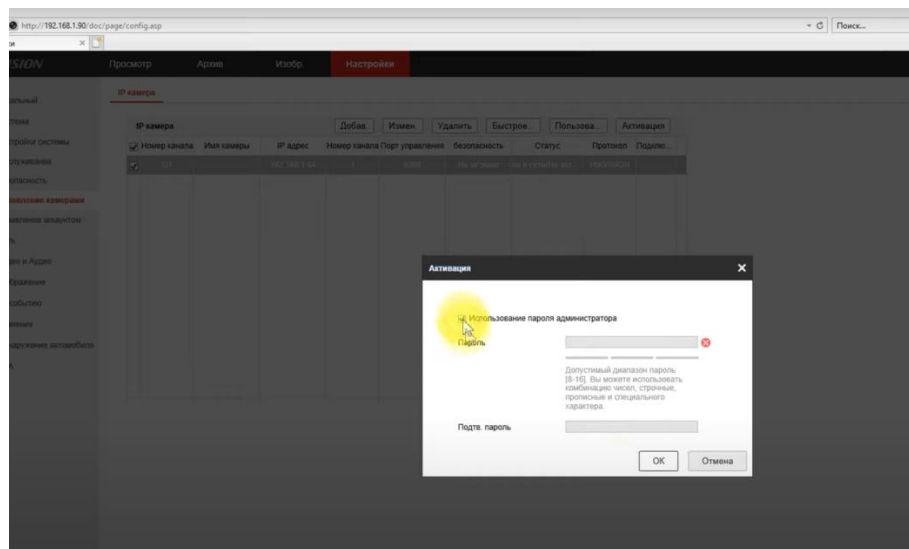


Рисунок 3.18 – Активация добавленной камеры

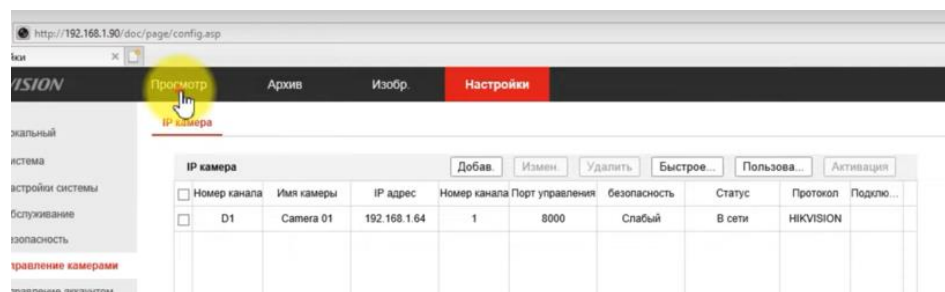


Рисунок 3.19 – Статус добавленной камеры

Аналогичным чином додаємо всі камери підсистеми.

Налаштуємо доступ до камер через мережу Інтернет. Для цього виконаємо налаштування наведені на рисунку 3.20.

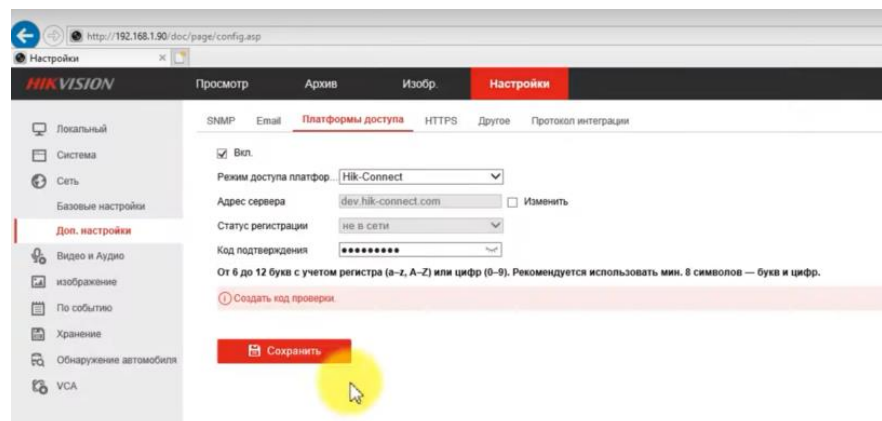


Рисунок 3.20 – Налаштування доступу до реєстратора через інтернет

Налаштування підсистеми відеоспостереження на цьому завершено.

Перейдемо до налаштування охоронної та пожежної підсистем. Пожежні спринклери є автономними і потребують лише підведеного до них водопостачання, тому налаштування для них не потрібні.

Для підключення інших пристроїв будемо використовувати додаток Ajax Security Systems. На початку створення системи в додатку необхідно додати керуючий пристрій – хаб. Додавання хабу, як і інших пристроїв буде здійснюватись шляхом сканування QR-коду в додатку.

Після додавання хабу переходимо до підключення датчиків до нього. Почергово відскановуємо наявні в кожній кімнаті датчики, підключаємо ретранслятор та додаємо вуличні датчики відкриття хвіртки та воріт. Оскільки в системі багато однотипних датчиків, то використовуємо відповідне іменування для них, щоб однозначно ідентифікувати пристрій.

Наступним кроком, для полегшення моніторингу та керування, розділимо наявні пристрої на групи відповідно до їх розташування.

Налаштовуємо параметри кожного датчика відповідно до потреб і розташування та одразу проводимо тестову їх перевірку. Після чого переходимо до створення сценаріїв.

Сценарії будуть наступні:

1. При постановці та знятті системи з охорони на мобільний пристрій власників приходитимуть сповіщення про дані дії.

2. Якщо під час того, як у системі увімкнено режим охорони датчики руху виявлять рух, то власник системи отримає спочатку сповіщення, а потім й фото з датчиків руху.

3. Якщо пожежний датчик виявить дим, або ж різку зміну температури автоматично буде увімкнено сирену, а також вимкнено електроживлення будинку за допомогою силового реле. Також при пожежі автоматично увімкнуться спринклери у місці виявлення вогню.

4. При невірному введенні коду зняття системи з охорони систему буде на деякий час заблоковано, а власники отримають відповідне сповіщення у мобільному додатку.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

5. Якщо спрацюють датчики відкриття дверей та вікон в час, коли система знаходиться в режимі охорони, то власники отримають відповідне сповіщення. Аналогічні дії будуть виконані при спрацюванні датчика розбиття скла.

Постановка системи на охорону та її зняття з даного режиму відбуватиметься трьома способами:

- За допомогою мобільного додатку власників.
- За допомогою охоронної клавіатури.
- За допомогою спеціального керуючого пульта.

Основні налаштування системи безпеки проведено, залишається лише протестувати її роботу.

3.3 Тестування функціоналу окремих підсистем та системи в цілому

Проведемо дослідження роботи системи за різних сценаріїв подій.

Сценарій 1. Власники покинули будинок та залишили його на охороні. Зловмисник скориставшись моментом вирішив проникнути на територію. Перелізши через паркан зловмисник зламав вікно та проникнув в будинок.

В той час, коли було зламано вікно власник отримав сповіщення через систему безпеки, після чого в кімнаті, в яку проникнув зловмисник спрацював датчик руху та надіслав власникові фото. Отримавши сповіщення власник викликав поліцію і зловмисника успішно було затримано.

Сценарій 2. Власник будинку зранку поспішаючи на роботу залишив увімкненою праску. Від нагрівання тканина під праскою загорілась і почалась пожежа.

Датчик виявив загорання і миттєво відправив сповіщення власникові, увімкнув сирену, а також система за допомогою силового реле знеструмила будинок. Також увімкнулись спринклери та пожежу було ліквідовано.

Сценарій 3. Зловмисники вирішили вимкнути електропостачання будинку шляхом перерізання дроту, що йшов від електромережі до будинку. Перерізавши дріт вони перелізли через паркан і розбили вікно.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

Втративши основне живлення будинок автоматично перейшов на резервне джерело. Система безпеки після вимкнення живлення продовжила працювати в штатному режимі, оскільки має батареї для автономного живлення. Після розбиття скла датчик спрацював та надіслав сповіщення на пристрої власників. Датчик руху зафіксував проникнення, а також надіслав фото зломисників власникам будинку. Власники викликали поліцію і зломисників було затримано.

Сценарій 4. Зломисники шляхом соціальної інженерії отримали код доступу від системи безпеки. Перелізши через паркан вони за допомогою охоронної клавіатури зняли систему з охорони та зайшли в будинок.

Після зняття системи з охорони власники будинку отримали відповідне сповіщення на мобільні пристрої. Підключившись до камер всередині будинку вони зафіксували зломисників та викликали поліцію, яка виконала їх затримання.

Сценарій 5. Зломисники непомітно перебрались через паркан на територію приватної власності та захопили власника, який тільки вийшов з будинку в заручники та змусили зняти систему з охорони. Власник системи мав в кишені непомітний пульт керування та натиснув тривожну кнопку, за допомогою якої викликав поліцію, яка звільнила його та затримала зломисників.

3.4 Висновки з розділу 3

В розділі 3 було підібрано та обґрунтовано вибір відповідних компонентів для організації роботи системи. Були пояснені відповідні технічні рішення та пропозиції.

Систему було реалізовано за допомогою комбінованого підходу. Підсистему відеоспостереження було реалізовано на пристроях компанії Hikvision, а охоронну та пожежну підсистеми реалізовано пристроями компанії Ajax, а також автономними спринклерами. Наведено сценарії реагування системи на можливі вторгнення.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

ВИСНОВКИ

У даній роботі було проведено аналіз існуючих підходів реалізації систем безпеки, підходів до їх побудови, описано переваги та недоліки кожного з них, які було враховано при подальшій розробці системи.

Також в даній роботі було спроектовано систему безпеки приватного домоволодіння. Було проведено розробку підсистем та схем розміщення пристроїв у них.

А також було проаналізовано апаратне забезпечення, підібрано та обґрунтовано вибір відповідних компонентів для організації роботи системи. Відповідні реалізовані технічні рішення та пропозиції були пояснені та представлені ключові моменти їх налаштування.

Розроблена у ході виконання кваліфікаційної роботи система може використовуватися у приватних будинках а також може бути покращена шляхом використання вдосокналених пристроїв та датчиків.

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Охоронна система Ajax – сигналізація та smart-системи | Офіційний сайт. Ajax Systems. URL: <https://ajax.systems/ua/>.
2. Gillis A. S. What is iot (internet of things) and how does it work? - definition from techtarget.com. IoT Agenda. URL: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>.
3. Підключення до ПЦС | служба підтримки ajax systems. Служба підтримки Ajax Systems. URL: <https://support.ajax.systems/uk/for-pro/cms-connection/>.
4. Радіотехнологія jeweller | ajax systems. Ajax Systems. URL: <https://ajax.systems/ua/jeweller/>.
5. Сценарії | служба підтримки ajax systems. Служба підтримки Ajax Systems. URL: <https://support.ajax.systems/uk/for-users/scenarios/>.
6. Таблиця відповідності пристроїв Ajax охоронним стандартам. Ajax Systems. URL: <https://ajax.systems/ua/standards/>.
7. Building security and personal safety / ed. by Association of Research Libraries. Systems and Procedures Exchange Center. Washington, D.C : Office of Management Services, Association of Research Libraries, 1989. 141 p.
8. Cassidy T., Books N. Cybersecurity and cyberwar: challenges and solutions. Independently Published, 2018.
9. Digital video surveillance and security. Elsevier, 2014. URL: <https://doi.org/10.1016/c2013-0-00650-0> (date of access: 25.06.2023).
10. Granzer W., Praus F., Kastner W. Security in building automation systems. IEEE transactions on industrial electronics. 2010. Vol. 57, no. 11. P. 3622–3630. URL: <https://doi.org/10.1109/tie.2009.2036033> (date of access: 25.06.2023).
11. Hillstrom S. B. The smart approach to home renovation (smart approach). Creative Homeowner, 2007. 224 p.
12. Hoffman B. Ajax security. Upper Saddle River, NJ : Addison-Wesley, 2008. 470 p.
13. Hub 2 plus | служба підтримки ajax systems. Служба підтримки Ajax Systems. URL: <https://support.ajax.systems/uk/central-units/hub-2-plus/>.

		Костюк Ю. В.			<i>КІК.КР.Б - 125 - 09 - 173</i>	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

14. Johnson B. R. Principles of security management. Prentice Hall, 2004. 488 p.
15. Lawson-Smith P. Building security systems. Wiring installations and supplies. 1985. Vol. 1985, no. 22. P. 17. URL: <https://doi.org/10.1049/wis.1985.0004> (date of access: 25.06.2023).
16. Maekawa M. Operating systems: advanced concepts. Menlo Park, Calif : Benjamin/Cummings Pub. Co., 1987. 414 p.
17. MotionCam (phod) | служба підтримки ajax systems. Служба підтримки Ajax Systems. URL: <https://support.ajax.systems/uk/indoor-security/motioncam-phod/>.
18. Muller P., Chen H.-H., Hu R. Q. Security in wireless networks and systems. Wiley & Sons, Incorporated, John, 2025.
19. Personnel protection: residential security. Elsevier, 2014. URL: <https://doi.org/10.1016/c2013-0-14166-9> (date of access: 25.06.2023).
20. Talmadge C., Sechser T. S., Narang N. Emerging technologies and international security. Taylor & Francis Group, 2021.

		Костюк Ю. В.			<i>КІК.КР.Б - 125 - 09 - 173</i>	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

ДОДАТКИ

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Технічні характеристики реєстратора Hikvision DS-7316HUNI-K4

- Кількість каналів: 16 каналів
- Вхідний/вихідний інтерфейс: HDMI, VGA, BNC
- Відеоформат: H.265+/H.265/H.264+/H.264
- Відеовходи: 16 каналів BNC
- Відеовиходи: 1 HDMI, 1 VGA, 1 BNC
- Роздільна здатність відео: до 4K (3840x2160) при 8 Мп
- Аудіовходи/виходи: 1/1 RCA
- З'єднання з мережею: 1 RJ-45 10/100/1000 Mbps Ethernet
- Зберігання: до 8 SATA-жорстких дисків з загальною ємністю до 64 ТБ
- USB-інтерфейси: 2 порти USB 2.0, 1 порт USB 3.0
- Підтримка мережевих протоколів: TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, NFS, iSCSI, UPnP™, HTTPS
- Операційна система: Embedded Linux
- Живлення: 100-240 В перемінного струму
- Споживана потужність: ≤ 20 Вт (без жорсткого диска)
- Робоча температура: -10°C до $+55^{\circ}\text{C}$
- Розміри (ШхВхГ): $445 \times 390 \times 70$ мм
- Вага: ≤ 5 кг

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - 13	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Технічні характеристики сховища даних Synology 2Bay DS223

- Кількість отворів для жорстких дисків: 2
- Тип жорстких дисків: 3.5" або 2.5" SATA HDD або SSD
- Максимальна ємність жорстких дисків: До 36 ТБ (2 x 18 ТБ)
- Процесор: 64-бітний 4-ядерний процесор Intel Celeron J4025 з тактовою частотою 2.0 ГГц
- Оперативна пам'ять: 2 ГБ DDR4, можливість розширення до 6 ГБ (2 ГБ + 4 ГБ)
- Роз'єми: 2 x RJ-45 1GbE LAN порти, 2 x USB 3.2 Gen 1 порти
- Розширення: Можливість підключення додаткових жорстких дисків за допомогою розширювальних одиниць Synology
- Підтримка RAID: RAID 0, RAID 1, JBOD
- Операційна система: DiskStation Manager (DSM)
- Розміри (ВхШхГ): 165 x 100 x 226 мм
- Вага: 1.3 кг (без жорстких дисків)

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Технічні характеристики камери Hikvision DS-2CE56D0T-IRMMF(C)

- Тип камери: аналогова камера
- Роздільна здатність: 2 мегапікселі (1920 x 1080)
- Тип матриці: CMOS
- Розмір матриці: 1/2.7"
- Мінімальна освітленість: 0.01 лк (F1.2, AGC вкл.)
- Об'єктив: фіксований об'єктив 3.6 мм
- Кут огляду: 86.5°
- ІК-підсвічування: до 20 метрів
- Корпус: металевий корпус, вандалозахищений
- Режими день/ніч: автоматичний (ICR)
- Захист від вологи та пилу: IP67
- Підтримка системи відеозапису: HDTVI/AHD/CVI/CVBS
- Напруга живлення: 12 В постійного струму
- Споживана потужність: до 4 Вт
- Робоча температура: -40°C до 60°C
- Вага: близько 260 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Технічні характеристики камери Hikvision DS-2CE16D0t-IT5E

- Розширення: 2 мегапікселі (1920 x 1080 пікселів)
- Тип сенсора: 1/2.7" прогресивний CMOS
- Об'єктив: фіксований об'єктив 2.8 мм, з фокусною відстанню 2.8 мм
- Чутливість: 0.01 люкс з F1.2
- Швидкість затвора: 1/25(1/30) с до 1/50,000 с
- Функції денного/ночі: ІЧ-підсвічування з досягом до 40 метрів
- Функції захисту: IP67 (водонепроникність), IK10 (стійкість до удару)
- Сигнал/шум: >62 дБ
- Коефіцієнт перекладу зображення: 2D DNR, 3D DNR
- Відеовихід: 1 HD-TVI вихід BNC (1920 x 1080p)
- Живлення: 12 В постійного струму
- Споживана потужність: Макс. 4.5 Вт
- Робоча температура: -40°C до 60°C
- Розміри: 86.7 мм x 81.6 мм x 226 мм
- Вага: Приблизно 680 грамів

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Технічні характеристики Ajax Hub 2 Plus

- Комунікація: Ethernet, GSM, Wi-Fi, Bluetooth
- Максимальна кількість підключених пристроїв: до 200
- Діапазон дистанції комунікації: до 2 км у відкритому просторі
- Керування пристроями через мобільний додаток (iOS та Android)
- Вбудований резервний акумулятор: 100 часів автономної роботи при відсутності живлення
- Можливість підключення до центральної станції охоронної організації
- Захист від взлому, переривання зв'язку та перенапруги
- Підтримка режимів охорони, пожежної сигналізації та контролю доступу
- Вбудований годинник реального часу
- Можливість оновлення прошивки для отримання нових функцій і виправлення помилок

		Костюк Ю. В.			КІК.КР.Б – 125 – 09 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Технічні характеристики Ajax MotionCam

- Тип пристрою: Бездротовий детектор руху з фотофіксацією
- Технологія зв'язку: Бездротовий радіоканал Jeweller
- Дальність зв'язку: До 1700 метрів в прямій видимості
- Частотний діапазон: 868.0-868.6 МГц
- Фотокамера: Вбудована цифрова камера з можливістю фотофіксації
- Роздільна здатність фотокамери: 640x480 пікселів
- Кут огляду фотокамери: 88.5°
- Чутливість детектора руху: Налаштовується в діапазоні 1-3 м/с
- Інтелектуальні фільтри: Фільтрація фальшивих спрацювань (наприклад, від домашніх тварин або штучного освітлення)
- Джерело живлення: Вбудована літій-іонна батарея
- Час роботи в автономному режимі: До 4 років
- Захист від зламу: Захищений від розкриття, зняття і перешкоджання передачі сигналу
- Робоча температура: Від -10°C до +40°C
- Габаритні розміри: 205 x 95 x 60 мм
- Вага: 193 грами

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Технічні характеристики Ajax DoorProtect

- Тип пристрою: Бездротовий дверний/віконний датчик
- Сумісність: Сумісний з Ajax Hub та Ajax Hub Plus
- Зона виявлення: 2 магнітних контакти (для дверей або вікон) та 1 додатковий вхід (датчик розриву)
- Бездротова технологія: Jeweller (868/915 МГц)
- Радіус дії: До 2 000 м (в відкритому просторі)
- Частота передачі даних: Кожні 12-300 секунд
- Тип сповіщення: Акустичний сигнал, сповіщення на мобільний телефон через мобільний додаток Ajax
- Ступінь захисту: IP50 (захист від пилу, обмежений захист від води)
- Джерело живлення: Вбудована літій-іонна батарея CR2032
- Тривалість роботи батареї: До 7 років (при нормальному використанні)
- Робоча температура: Від -10°C до +40°C
- Розміри: 20 x 90 x 20 мм
- Вага: 25 грам
- Колір: Білий

		Костюк Ю. В.			KIK.KP.B - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Технічні характеристики Ajax DoorProtect Plus

- Тип: Бездротовий магнітоконтантний датчик
- Використання: Захист дверей та вікон у системі безпеки
- Дальність зв'язку: До 1200 метрів у відкритому просторі
- Частота роботи: 868.0-868.6 МГц
- Метод передачі сигналу: Двостороння радіокомунікація з підтвердженням отримання сигналу
- Захист від зламу: Датчик виявляє відчинення дверей або вікон, а також спроби зламу
- Швидкість реакції: 0,15 секунди
- Живлення: Вбудована літій-полімерна батарея CR123A (3 В)
- Час роботи батареї: До 5 років при звичайному використанні
- Комплектація: Датчик, магніт, кріплення для установки
- Розміри (Д х Ш х В): 20 х 90 х 20 мм
- Вага: 27 грамів

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

Технічні характеристики Ajax GlassProtect

- Тип пристрою: Бездротовий датчик розбиття скла
- Використовується в системах безпеки для виявлення незаконного вторгнення через розбиття скляних поверхонь
- Робоча частота: 868.0-868.6 МГц
- Максимальна відстань зв'язку з центральною станцією: до 1,200 м (в прямій видимості)
- Метод сповіщення: відправка безпроводового сигналу до центральної станції або іншого підключеного пристрою
- Система захисту від зламу: пристрій має вбудований алгоритм захисту, який сповіщає про спроби впливу на нього (наприклад, розбиття або від'єднання)
- Спеціальна технологія: аналізує частотний спектр і шумове середовище для забезпечення надійної роботи без спотворень
- Живлення: вбудована літієва батарея CR123A
- Робочий час без заміни батареї: до 7 років
- Додаткові функції: можливість встановлення датчика на вікні або дзеркалі, звукове оповіщення про активацію, можливість підключення до смартфона для отримання повідомлень через мобільний додаток
- Розміри: 20 x 90 мм
- Вага: 35 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Технічні характеристики Ajax ReX 2

- Тип пристрою: Бездротовий реле-розширювач сигналу
- Використовується в системах безпеки для підвищення зон покриття та забезпечення стабільного зв'язку між бездротовими пристроями і центральною станцією
- Робоча частота: 868.0-868.6 МГц
- Максимальна відстань зв'язку з центральною станцією: до 1,800 м (в прямій видимості)
- Метод сповіщення: передача безпроводових сигналів між бездротовими пристроями і центральною станцією
- Система захисту від зламу: пристрій має вбудований алгоритм захисту, який сповіщає про спроби впливу на нього (наприклад, розбиття або від'єднання)
- Спеціальна технологія: аналізує частотний спектр і шумове середовище для забезпечення надійної роботи без спотворень
- Живлення: вбудована літієва батарея CR123A
- Робочий час без заміни батареї: до 5 років
- Додаткові функції: можливість підключення зовнішніх датчиків і сирен, можливість керування реле для включення/виключення пристроїв, підтримка алгоритму унікального ідентифікатора для запобігання підробці
- Розміри: 80 x 80 x 35 мм
- Вага: 97 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

Технічні характеристики Ajax KeyPad Plus

- Тип пристрою: Бездротова клавіатура для управління системою безпеки
- Використовується для активування та деактивування системи безпеки, введення підтверджувальних кодів та керування режимами безпеки
- Робоча частота: 868.0-868.6 МГц
- Максимальна відстань зв'язку з центральною станцією: до 1,300 м (в прямій видимості)
- Метод сповіщення: відправка безпроводового сигналу до центральної станції або інших підключених пристроїв
- Захист від підбору коду: вбудований алгоритм захисту від підбору паролю або підслуховування
- Дисплей: кольоровий сенсорний TFT-дисплей з підсвічуванням
- Клавіші: механічні клавіші з підсвічуванням
- Живлення: вбудована літієва батарея CR2032
- Робочий час без заміни батареї: до 2 років
- Додаткові функції: можливість встановлення на стіну або монтаж на столі, можливість програмування до 50 користувачів з індивідуальними кодами доступу
- Розміри: 150 x 102 x 13 мм
- Вага: 173 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

Технічні характеристики Ajax FireProtect Plus

- Тип пристрою: Бездротовий пожежний датчик
- Використовується в системах безпеки для виявлення пожежі та викиду диму
- Робоча частота: 868.0-868.6 МГц
- Максимальна відстань зв'язку з центральною станцією: до 1,300 м (в прямій видимості)
- Метод сповіщення: відправка безпроводового сигналу до центральної станції або іншого підключеного пристрою
- Тип сповіщення: активує внутрішню сирену, сповіщення на смартфон через мобільний додаток, відправка SMS або електронної пошти
- Чутливість: виявлення диму за рахунок часткового викиду продуктів горіння
- Інтелектуальні алгоритми: використовуються для зниження ймовірності випадкових спрацьовувань та підвищення надійності розпізнавання пожежі
- Живлення: вбудована літієва батарея CR2
- Робочий час без заміни батареї: до 4 років
- Додаткові функції: можливість підключення до смартфона для отримання повідомлень через мобільний додаток, самоперевірка стану пристрою, пам'ять історії спрацьовувань
- Розміри: 132 x 132 x 31 мм
- Вага: 222 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Технічні характеристики Ajax WallSwitch

- Тип пристрою: Бездротовий вимикач освітлення
- Використовується для керування освітленням у приміщенні
- Робоча частота: 868.0-868.6 МГц
- Максимальна відстань зв'язку з центральною станцією: до 1,300 м (в прямій видимості)
- Метод керування: безпроводове управління освітленням за допомогою вимикача
- Зворотний зв'язок: підтвердження виконання команди вимикачем
- Завдяки релейному виходу можливе керування електромагнітними замками та розетками
- Захист від перевантажень та короткого замикання
- Живлення: вбудована літієва батарея CR2032
- Робочий час без заміни батареї: до 5 років
- Додаткові функції: можливість налаштування різних сценаріїв освітлення, інтеграція з іншими системами безпеки Ајах, проста установка та налаштування
- Розміри: 41 x 32 x 14 мм
- Вага: 20 г

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

Технічні характеристики спринклера RAPIDROP RD021

- Тип пристрою: Автоматичний пожежний спринклер
- Використовується для пожежогасіння та контролю пожежі у промислових та комерційних приміщеннях
- Максимальний робочий тиск: 12 бар
- Максимальна температура робочого середовища: 68°C
- Матеріал корпусу: Мідь або нержавіюча сталь
- Розмір різьблення: 1/2", 3/4", 1" або 1 1/4"
- Витрата води: від 56 до 265 л/хв (залежно від типу і розміру спринклера)
- Клас пожежі: А, В, С, D, Е, F
- Монтаж: може бути встановлений на стелях або на вертикальних поверхнях
- Особливості: може бути обладнаний температурними фішками, що реагують на підвищення температури, а також об'ємними фішками для детектування пожежі відповідно до встановленого порогу
- Сертифікація: відповідає стандартам FM, LPCB, UL, VdS, CE

		Костюк Ю. В.			КІК.КР.Б - 125 - 09 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		74