МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютеризованих систем управління

«До захисту допущено»
Завідувач кафедри КСУ
_____ Петро ЛЕОНТЬЄВ
_____ _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня __бакалавр__

зі спеціальності 151 – Автоматизація та комп'ютерно-інтегровані технології
освітньо-професійної програми
«Комп'ютеризовані системи управління та робототехніка»
на тему: «Автоматизована охоронна система для комерційних приміщень»

Здобувача(ки) групи СУ-91 Бєльский Андрій Сергійович

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

_____ Андрій БЄЛЬСЬКИЙ
(підпис)

Керівник: доцент кафедри КСУ, к.ф-м. н., доцент, В'ячеслав ЖУРБА _____
(посада, науковий ступінь, вчене звання, Ім'я ПРІЗВИЩЕ) (підпис)

Суми – 2023

Ном.поз	Формат	Позначення	Найменування	Кількість аркушів	№ екз.	Примітки
			Документація загальна			
			Застосована			
1	А4		Завдання кафедри	2		
			Новорозроблена			
2	А4	ТЗ	Технічне завдання	5		
3			Анотація	1		
4	А4	СУ-91 6.151.01 ПЗ	Пояснювальна записка	71		
			Документація конструкторська			
			Новорозроблена			
5	А4	СУ-91 6.151.01 Е3	Електрична принципова схема	1		
6	А4	СУ-91 6.151.01 П5	Схема підключення	1		
7	А4	СУ-91 6.151.01	План-проєкт приміщення	1		

					СУ-91.6.151.01.ДП			
Змн.	Арк.	№ докум.	Підпис	Дата				
		Бельский А.С.			Автоматизована охоронна система для комерційних приміщень Відомість проєкту	Літ.	Арк.	Аркушів
		Журба В.О.						
Реценз.						СумДУ, СУ-91		
Н. Контр.								
Затверд.		Леонтьев П.В.						

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютеризованих систем управління

ЗАТВЕРДЖУЮ:
Зав. кафедри КСУ
_____Петро ЛЕОНТЬЄВ
_____ _____ 2023 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра здобувачу вищої освіти
Бєльському Андрію Сергійовичу

1. Тема кваліфікаційної роботи: Автоматизована охоронна система для комерційних приміщень.

2. Термін здачі студентом закінченої роботи " 10 " червня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: звіт з переддипломної практики, наукові публікації, статті, технічна документація та перелік літературних джерел з матеріалом про подібні системи.

4. Зміст кваліфікаційної роботи (питання, що підлягають розробленню):

- Загальні принципи захисту об'єктів інженерно-технічних засобів охорони
- Загальні відомості про інтегровану охоронну систему Дунай
- Принцип роботи охоронної системи Дунай

5. Перелік графічних матеріалів: 12 рисунків, 17 таблиць, 3 додатки.

6. Календарний план виконання роботи

Номер етапу	Зміст етапу виконання роботи	Термін виконання
1	Ознайомлення із завданням.	24.02.2023–03.03.2023
2	Ознайомлення з загальними принципами захисту об`єктів інженерно-технічних засобів охорони. Аналіз існуючих охоронних систем	04.03.2023–25.03.2023

3	Розробка технічного завдання. Ознайомлення з охоронною системою Дунай	26.03.2023–14.04.2023
4	Визначення загальних відомостей про інтегровану охоронну систему Дунай	05.04.2023–25.04.2023
5	Аналіз принципу роботи охоронної системи Дунай	26.04.2023–15.05.2023
6	Оформлення дипломного проекту та технічної документації.	10.06.2023

7. Дата видачі завдання " 24 " лютого 2023 р.

Керівник проекту:

доцент кафедри КСУ,
к.ф-м. н., доцент В’ячеслав ЖУРБА

Здобувач:

студент гр. СУ-91 Андрій БЄЛЬСЬКИЙ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра комп’ютеризованих систем управління

ТЕХНІЧНЕ ЗАВДАННЯ

на проектування автоматизованої охоронної системи для комерційних приміщень.

Розробник:
студент групи СУ-91 Андрій БЄЛЬСЬКИЙ

Погоджено:
к.ф.-м.н., доцент В’ячеслав ЖУРБА

Суми – 2023

1. ***Назва і галузь застосування:***

Автоматизована охоронна система для комерційних приміщень. Галузь безпеки та захисту.

2. ***Підстави для проектування*:**

Наказ ректора Сумського державного університету № 0263 VI від “14” березня 2023р.

3. ***Загальний опис об’єкта автоматизації:***

БВН В.2.5-78.11.01-2003 «Системи сигналізації охоронного призначення», ГСТУ 78.11.001-98 «Укріпленість об’єктів, що охороняються за допомогою пультів централізованого спостереження Державної служби охорони.

4. ***Основні частини системи та структурна схема:***

Система охоронної сигналізації призначена для попередження про несанкціоноване проникнення в приміщення через вразливі місця: двері, вікна і некапітальні стіни.

5. ***Опис блоків системи керування* :**

- *Блок живлення*
- *Блок підключення*
- *Блок сигналізації*
- *Блок підтвердження інформації*

6. ***Опис алгоритмів та режимів роботи системи***.

Система охоронної сигналізації призначена для попередження про несанкціоноване проникнення в приміщення через вразливі місця: двері, вікна і некапітальні стіни.

7. ***Умови експлуатації системи керування:***

Умови експлуатації технологічного устаткування процесу адсорбції:

а) температура навколишнього середовища – від мінус 20 до 50ºС;

б) відносна вологість до 100% при температурі до 35ºС;

в) атмосферний тиск від 84 до 106,7 кПа (від 630 до 800 мм рт. ст.);

г) постійна вібрація з частотою до 30 Гц з амплітудою не більше за 0,1 мм;

д) тип навколишнього середовища – невибухонебезпечні пожежонебезпечні зони відкритих промплощадок приміщень класу Д.

Умови експлуатації технічних засобів, що встановлюються в приміщенні на щитах керування:

а) температура навколишнього середовища – від плюс 5 до 50ºС б) відносна вологість до 80% при температурі до 25ºС;

в) атмосферний тиск від 84 до 106,7 кПа (від 630 до 800 мм рт. ст.);

г) постійна вібрація з частотою до 30 Гц з амплітудою не більше за 0,1 мм.

8. *Технічні вимоги*:

Вимоги за призначенням

- Обладнання пожежної та охоронної сигналізації повинно бути розміщено в офісному приміщенні відповідно до плану.
- Система повинна забезпечувати формування та передачу на пульт централізованного спостереження а також через мобільний додаток сигналу тривоги в разі несанкціонованого проникнення в будь-яке приміщення охороняємого об’єкту.
- Для побудови автономної чи пультової системи охорони з функціями керування автоматикою в системі повинен бути встановлений ППК.
- В залежності від вимог об’єкту, що охороняється, до ППК повинні підключаються провідні та/або безпровідні сповіщувачі, оповіщувачі, модулі розширення та пристрої ідентифікації доступу.
- Керування системою повинне здійснюватися з локальних пристроїв ідентифікації доступу (клавіатури, зчитувачі ключів Touch Memory (ТМ), радіобрелки та дистанційно, через мережу internet, при використанні мобільного застосунку Control NOVA II.

- ППК повинен передавати інформацію про стан системи на ПЦС, мобільний застосунок Control NOVA II, SMS-повідомленнями та контрольним дзвінком на визначені номери телефонів.
- ППК повинен забезпечувати безперервну роботу в приміщеннях з регульованими кліматичними умовами при відсутності прямого впливу кліматичних факторів зовнішнього середовища.
- Повинна забезпечуватися робота ППК через мережу GSM (GPRS) по технології 2G. Модуль повинен надавати можливість передачі SMS-повідомлень та здійснення контрольного дзвінка на мобільні телефони користувачів.
- Основне живлення повинне виконуватися від мережі змінного струму напругою 220 В (+22 В,-33 В), частотою 50 Гц 1.
- Споживана потужність (без врахування зовнішніх сповіщувачів і оповіщувачів), - не більше 25 ват.
- Система повинна мати світлову та звукову індикацію спрацювань сиситеми охоронно-пожежної сигналізації.
- В системі повинна забезпечуватися спорядження приміщень індивідуальними кодами з мобільного додатку в залежності від виданих повноважень.
- При зникненні напруги у мережі електроживлення, система автоматично повинна переходить на живлення від вбудованої акумуляторної батареї.
- Вимоги з життєздатності та стійкості до зовнішніх впливів і чинників
- Обладнання відноситися до групи 4.2 виконання УХЛ ГОСТ 15150.

Вимоги по надійності

- Система охоронної та пожарної сигналізації повинно мати середній час наробітку на відмову не менш 50000 годин.
- Повний середній ресурс обладнання повинен бути не менш 100000 годин,
- Повний термін служби до списання - не менш 15 років.
- Вимоги по ергономіці і технічній естетиці

- Конструкція складових системи повинна відповідати вимогам по ергономіці й технічній естетиці, викладеним у розділі 1.2 ГОСТ 20.39.108-85.

9. ***Стадії та етапи проектування*****:**

Номер етапу	Зміст етапу проектування	Термін виконання
1	Ознайомлення із завданням.	21.02.2023–01.03.2023
2	Ознайомлення з загальними принципами захисту об`єктів інженерно-технічних засобів охорони. Аналіз існуючих охоронних систем	02.03.2023–16.04.2023
3	Розробка технічного завдання. Ознайомлення з охоронною системою Дунай	16.04.2023–19.04.2023
4	Визначення загальних відомостей про інтегровану охоронну систему Дунай	20.04.2023–25.04.2023
5	Аналіз принципу роботи охоронної системи Дунай	25.04.2023–05.05.2023
6	Технічне оформлення проекту.	06.05.2023–28.05.2023

10. ***Додатки*****:**

Додаток А. Електрична принципова схема

Додаток Б. Схема підключення

Додаток В. План-проєкт приміщення

АНОТАЦІЯ

Тема роботи: Автоматизована охоронна система для комерційних приміщень

Автор: Бєльський Андрій Сергійович; Сумський державний університет; 4 курс; Суми.

Науковий керівник: Журба В’ячеслав Олегович; доцент кафедри КСУ кандидат фізико-математичних наук, доцент.

Робота містить вступ, чотири розділи, загальним обсягом 71 сторінку, 12 рисунків, 17 таблиць, 16 джерел.

У процесі роботи було проведено ознайомлення із сучасними пристроями охоронно-пожежної сигналізації та підбір оптимального обладнання для фінансової установи.

В результаті дослідження було спроектовано систему охоронно-пожежної сигналізації, що відповідає всім сучасним вимогам та гнучкості конфігурації. Основні конструктивні, технологічні та техніко-експлуатаційні характеристики: оперативний зв'язок приймально-контрольного приладу з пунктом централізованого спостереження позавідомчою охороною під час спрацьовування датчиків.

Ступінь впровадження: проект виконаний на замовлення фінансової установи.

Область застосування: охоронно-пожежна сигналізація фінансової установи.

Ключові слова: охоронна система, сигналізація, Дунай.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет електроніки та інформаційних технологій
Кафедра комп'ютеризованих систем управління

ЗАТВЕРДЖУЮ
Завідувач кафедри КСУ
_____ Петро ЛЕОНТЬЄВ
_____ _____ 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту
зі спеціальності 151 – Автоматизація та комп'ютерно-інтегровані технології
на тему:
«Автоматизована охоронна система для комерційних приміщень»

Керівник проекту:
к.ф.-м.н., доцент В'ячеслав ЖУРБА

Здобувач:
Студент групи СУ-91 Андрій БЄЛЬСЬКИЙ

Суми – 2023

ЗМІСТ

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

САК – Система автоматичного керування;

ВМ – виконуючий механізм;

ПЛК – програмований логічний контролер;

УГЗ - умовно-графічне зображення;

ТЗА – технічні засоби автоматизації;

ЛК – логічний контролер;

ЩК – щит керування;

SMD - surface mount device;

ІЧ – інфрачервоний;

МО – монтажний отвір;

ДП – друкована плата;

ДДП – двостороння друкована плата ;

ДМ – друкований монтаж;

УГП - умовне графічне позначення.

ВСТУП

Одним із найважливіших аспектів успішного функціонування підприємств, компаній, банків, магазинів та інших організацій є забезпечення належного рівня безпеки. У сучасних умовах це стає пріоритетним завданням через зростання злочинності, активізацію терористичних дій, збільшення кількості нещасних випадків та необхідність захисту новітніх інформаційних технологій. Засоби захисту людей і майна еволюціонували від простих методів фізичного захисту до сучасних систем безпеки.

У сучасних умовах все більше керівників усвідомлюють важливість безпеки та збільшують свої витрати на цей напрямок. Однак, зростання "невиробничих" витрат, зокрема на безпеку, ставить під сумнів ефективність традиційних підходів, основаних на використанні людського фактору. Тому виникає потреба в підвищенні рівня захисту і оптимізації систем безпеки фірми.

Таким чином, забезпечення безпеки стає важливою галуззю для бізнесу, оскільки допомагає забезпечити нормальне функціонування організацій і захистити їх від потенційних загроз.

Поняття безпеки включає різноманітні аспекти, такі як технічна укріпленість об'єкту, системи охорони, пожежна безпека, режим об'єкту та інформаційна безпека.

Технічна система охорони (ТСО) визначається як система, що ранньо виявляє загрози фірмі, такі як стихійні лиха, несанкціоноване проникнення порушників або помилкові дії обслуговуючого персоналу або клієнтів. Для виявлення та нейтралізації таких загроз застосовуються різні технічні засоби (ТЗ) та методи. Важливо правильно обрати оптимальні напрямки побудови такої системи, враховуючи особливості об'єкту та сучасні технології.

Одним з найпоширеніших варіантів є системи охоронно-пожежної сигналізації, які ефективно вирішують проблеми безпеки за допомогою технічних засобів. Проте найефективнішим є комплексний підхід до забезпечення безпеки за

допомогою інтегрованих систем. Вони включають системи охоронної та пожежної сигналізації, а також системи контролю та управління доступом та охоронного телебачення. В інтегрованих системах всі технічні засоби контролюються та керуються за допомогою передових комп'ютерних технологій та сучасних програмно-апаратних засобів.

Підготовка кадрів з відповідними навичками є необхідною для успішного встановлення та експлуатації сучасних систем безпеки на об'єктах. Монтаж інженерно-технічних засобів безпеки є складним технічним процесом. Від кваліфікації монтажників, їх знань сучасних монтажних технологій, робочих методів і вміння користуватися спеціалізованими інструментами і механізмами залежить якість і надійність функціонування систем безпеки об'єктів упродовж тривалого періоду, спрямованого на захист майна і безпеку людей від злочинних посягань і пожежі.

У сучасних ринкових умовах монтажники повинні не лише добре знати сучасні технології електромонтажу та вміло ними користуватися, але й глибоко вивчати технічні і конструктивні особливості технічних засобів систем безпеки, їх принципи побудови і функціонування, методи перевірки та безпечні методи монтажу.

Засоби навчання, такі як підручники та навчальні посібники, які відображають сучасний рівень розвитку систем безпеки, відіграють велику роль у забезпеченні належної якості підготовки фахівців. Проте багато з них обмежуються описом технічних характеристик конкретного обладнання. Виявляється, що існує недостатній кількісний обсяг підручників і навчальних посібників, які охоплюють загальні принципи побудови, функціонування, проектування, монтажу і експлуатації сучасних систем безпеки.

Головною **метою** даного дипломного проекту є розробка комплексної системи безпеки, аналіз доцільності використання різних засобів та огляд ринку систем безпеки з метою вибору найбільш підходящої системи та обладнання для конкретного об'єкту.

Для досягнення мети проектування комплексної системи охорони необхідно виконати наступні **завдання**:

- Аналіз потреб і вимог: Вивчення потреб та вимог, які стосуються безпеки об'єкта, включаючи захист майна і безпеку людей.
- Дослідження технічних можливостей: Оцінка різних технічних засобів і технологій, які можуть бути використані для створення системи охорони.
- Вибір оптимальних рішень: Визначення найбільш підходящих систем безпеки та обладнання, враховуючи особливості об'єкта, його ризики та потреби.
- Проектування системи: Розроблення детального проекту комплексної системи охорони, включаючи схеми, плани розташування засобів, комунікаційні системи та інші технічні аспекти.
- Монтаж і пуско-налагоджувальні роботи: Установка і налаштування технічних засобів, включення їх в роботу, перевірка функціональності та відповідності вимогам.
- Експлуатація і обслуговування: Забезпечення належної роботи системи охорони, проведення регулярного технічного обслуговування, навчання персоналу використовувати систему правильно та ефективно.

РОЗДІЛ 1. ЗАГАЛЬНІ ПРИНЦИПИ ЗАХИСТУ ОБЕКТІВ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ

1.1 Концептуальні питання забезпечення безпеки об`єкту

Для створення оптимальної та ефективної системи безпеки об'єкту, необхідно спочатку розробити обґрунтовану концепцію, яка визначатиме цілі захисту, потенційні загрози і ймовірність їх виникнення, а також основні стратегії для розв'язання завдань з охорони різних цінностей від аварій, природних катастроф та незаконних дій потенційних порушників.

Предметом захисту є конкретні цінності організації, які підлягають охороні за допомогою відповідної системи. Ці цінності включають:

- Людей: персонал об'єкту, відвідувачі та клієнти організації.
- Матеріальні та фінансові цінності: гроші, цінні папери, документи, обладнання.
- Конфіденційна інформація.

Пріоритети цих цінностей в значній мірі залежать від характеру діяльності організації.

Об'єктом захисту є фізичний простір, де знаходяться зазначені цінності. Він визначає потенційні дії порушників безпеки і, відповідно, заходи для запобігання загрозам безпеці організації.

Способи створення технічної системи безпеки значно залежать від характеристик приміщень та інженерно-технічних систем об'єкту, який підлягає захисту, їх відповідності нормативно-технічній документації з будівництва, вимогам безпеки та протипожежних правил. Також великий вплив на характеристики технічної системи безпеки має стадія, на якій знаходиться об'єкт - розробка проекту, будівництво, реконструкція або постійна експлуатація.

У кожній організації існують приміщення, які потребують особливого підходу до їх охорони. Серед таких приміщень першочергово виділяються:

- Кабінети керівництва фірми.
- Переговорні кімнати.

- Касові приміщення.
- Центр обчислювальної і телекомунікаційної мережі, відомий як "серверна".
- Приміщення АТС і комутаційного устаткування телефонної мережі.
- Приміщення з комутаційно-розподільною апаратурою інформаційно-телекомунікаційних систем (ІТКС) і систем безпеки.
- Базові приміщення систем інженерного забезпечення (СІЗ) - вентиляційна камера, електрощитова кімната, приміщення резервного електроживлення і диспетчерська служба.
- Приміщення служби безпеки фірми - центральний пост охорони, пост пожежної охорони.
- Архів паперових і електронних копій.

Найсуттєвіші технологічні приміщення, з урахуванням характеру бізнес-процесу в організації. Загрози безпеці компанії можна класифікувати таким чином: за природою появи - випадкові загрози та загрози, спричинені навмисними діями порушників; за відношенням до захищеного об'єкту: зовнішні та внутрішні загрози.

До випадкових загроз (зовнішніх та внутрішніх) відносяться стихійні лиха та катастрофи природного або техногенного характеру, аварії або порушення роботи систем, що забезпечують життєдіяльність об'єкту, а також помилкові дії персоналу та відмови устаткування. До зовнішніх загроз також входять криміногенні загрози, недобросовісна конкуренція, промислове шпигунство зловмисників, які діють з умислом. Загрози, спричинені навмисними діями порушників безпеки об'єкту (як зовнішніх, так і внутрішніх), проявляються у викраденні матеріальних цінностей, вандалізмі, вродительстві, саботажі, диверсіях і терорізмі. Основними мотивами таких загроз можуть бути незадоволення конкретним керівником, бажання самовиявитися, заздрість, корисливе прагнення отримати матеріальну або іншу вигоду, а також намір реалізувати свої політичні, релігійні та ідеологічні установки.

Внутрішні загрози включають зловмисні дії персоналу, які, як правило, виникають у зв'язку з соціально-психологічними та моральними проблемами.

Ініціаторами цього типу загроз зазвичай є самі співробітники або зовнішні структури, які спрямовують свої дії на підкуп персоналу.

Оцінка загроз, аналіз ризиків їх реалізації та прогнозування можливих збитків від кожного типу загроз є ключовим аспектом забезпечення безпеки компанії.

Принципи побудови та оптимізації системи технічного захисту об'єкту:

- Універсальність, яка передбачає, що всі рішення повинні бути стандартизовані та узгоджені.
- Комплексність, яка підкреслює, що застосовані методи та технічні засоби повинні бути взаємозалежними та доповнювати один одного за функціональними та технічними показниками.
- Розумна достатність, що означає, що заходи щодо забезпечення безпеки об'єкту повинні бути пропорційними можливим загрозам з точки зору фінансових, матеріально-технічних та кадрових ресурсів.
- Оперативність, яка вимагає надання пріоритету методам та засобам захисту, спрямованим на швидке виявлення та нейтралізацію можливих загроз.
- Адаптивність, що передбачає гнучке пристосування методів та засобів захисту до змін організаційних та технічних умов функціонування об'єкту.
- Безперервність та систематичність, що означають, що обрані рішення забезпечують ефективний цілодобовий захист об'єкту.
- Цілеспрямованість, яка полягає в акцентуванні зусиль на захисті найцінніших ресурсів компанії або найуразливіших зон об'єкту.
- Багаторубіжність, яка передбачає використання додаткових просторових рубежів безпеки або методів захисту для найбільш вразливих приміщень та зон об'єкту.
- Півноміцність створених меж безпеки.

- Послідовність в застосуванні відповідних методів та засобів при виявленні, відбитті та ліквідації загроз безпеці об'єкту (так звана компілярна безпека).
- Сумісність з існуючими системами.
- Простота, екологічна чистота та непомітність ("дружність"), що означають, що встановлена система не створює додаткових перешкод для нормального функціонування компанії, не вимагає високого рівня кваліфікації та тривалої підготовки персоналу, а також не завдає шкоди цінностям об'єкту, що захищаються.
- Невразливість, яка вказує на здатність протистояти спробам вивести систему з ладу.
- Правомірність, що означає, що всі застосовані заходи організаційного та технічного характеру є законними та юридично обгрунтованими.

Оптимальний підхід до створення системи технічного забезпечення об'єкту полягає у вживанні необхідних заходів з поступовим підвищенням ефективності всієї системи забезпечення безпеки, враховуючи виділені ресурси та пріоритети. При цьому слід ураховувати концептуальні положення забезпечення безпеки, особливості об'єкту та оперативну обстановку. Використання різних типів технічних систем безпеки, таких як системи контролю та управління доступом, пожежної та охоронної сигналізації, систем відеоконтролю, може сприяти досягненню високого рівня безпеки об'єкту. Розгортання таких систем зазвичай не вимагає великих фінансових витрат і базується на випробуваних технічних рішеннях. Варто пам'ятати, що обладнання та рішення, запропоновані підрядчиками, можуть бути обмежені їхніми знаннями та ресурсами. Враховуючи складність і вартість встановлення всіх необхідних систем, важливо уникати непотрібного дублювання функцій та забезпечити взаємодію між системами, щоб уникнути складнощів та обмежень у функціональності системи безпеки.

1.2 Опис об’єкту автоматизації

Система інженерно-технічного захисту територій та приміщень включає різноманітні пристрої, конструкції, апарати та вироби, які призначені для перешкоджання зловмисникам у досягненні їх цілей. Ці засоби можуть бути механічними, електромеханічними, електронними, електронно-оптичними, радіо- та радіотехнічними тощо, і призначені для заборони несанкціонованого доступу, проносу та інших злочинних дій.

Інженерно-технічні засоби фізичного захисту є ключовою складовою ефективності функціонування системи захисту об'єкту інформації. Вони здатні запобігти витоку інформації через ті канали, які не можуть бути захищені за допомогою технічних засобів виявлення та захисту. Наприклад, для захисту інформації від акустичних каналів, необхідно використовувати активні методи захисту, оскільки технічні засоби не можуть повністю запобігти витоку інформації через такі канали.

Для досягнення цих цілей використовуються пасивні методи за допомогою інженерно-технічних засобів фізичного захисту. Наприклад, у приміщеннях для проведення конфіденційних переговорів застосовуються пасивні методи, такі як звукоізоляція, яка досягається шляхом щільного закриття вікон та дверей з подвійними віконними рамами та додатковими тамбурами.

Ці інженерно-технічні засоби застосовуються для виконання наступних завдань:

- Охорона території підприємства та здійснення спостереження за нею.
- Захист будівель, внутрішніх приміщень та контроль над ними.
- Забезпечення безпеки обладнання, продукції, фінансів та інформації.
- Контрольований доступ до будівель та приміщень.

Усі фізичні засоби захисту об'єктів можна поділити на три категорії: засоби попередження, засоби виявлення та засоби нейтралізації загроз.Виходячи з цих уявлень та використовуючи раніше прийняту схему проведення декомпозиції, розглянемо структуру та склад засобів підсистеми інженерно-технічного захисту територій та приміщень та її елементів.

Підсистема попередження загроз містить два типи захисних засобів:

– Інженерні засоби фізичного захисту.
– Засоби контролю та управління доступом.

Інженерні засоби фізичного захисту включають:

– Природні та штучні бар'єри.
– Спеціальні конструкції для захисту периметру, проходів, вікон, дверей будівель і приміщень, а також сейфів і сховищ.
– Зони безпеки.

До природних бар'єрів відносяться:

– Нерівності території (рви, яри, скелі).
– Густий ліс та чагарники.
– Водні перешкоди.

Штучні бар'єри включають такі елементи:

– Бетонні або цегляні огорожі.
– Конструкції для обмеження швидкості руху транспортних засобів.
– Ґрати, сітчасті конструкції, металеві огорожі та інші види перешкод.

Також існують інженерні засоби, які створюють додаткові перешкоди, такі як колючий дріт, гострі металеві стрижні або бите скло, які встановлюються на огорожі. Можуть бути використані непомітні дротяні мережі, що створюють зону відчуження вздовж огорожі.

Варто відзначити, що на об'єктах з високим рівнем захисту застосовуються дві лінії штучних бар'єрів, розташовані на відстані 1 – 1,5 м один від одного. Також може використовуватись комбінація штучних і природних бар'єрів.

Спеціальні конструкції для периметрів, проходів, вікон та дверей приміщень, сейфів і сховищ включають:

– Дерев'яні або металеві двері (ворота).
– Вікна, які посилені різними способами.
– Металеві шафи, сейфи та сховища.

Ці структури повинні витримувати будь-які фізичні впливи, такі як механічні пошкодження, свердління, термічне та механічне різання, вибухи та інші, а також запобігати несанкціонованому доступу, такому як підробка ключів чи вгадування кодів. Одним з основних технічних засобів захисту проходів, приміщень, сейфів та сховищ є замки. Замки можуть бути:

- Прості механічні, які відкриваються (закриваються) механічним ключем, або електромеханічні, які відкриваються як механічним ключем, так і за допомогою електричного сигналу;
- Кодові, які можуть бути механічними або електронними з кодом (включаючи тимчасову затримку перед відкриванням).

Крім замків, надійність дверей (воріт) залежить від їх товщини, міцності матеріалу та способу кріплення дверної рами до стіни.

Вікна є одним з найбільш вразливих місць у системі інженерно-технічного захисту територій та приміщень. Їх зміцнюють двома основними способами:

- Використанням спеціального скла, яке відпоровує механічним ударом;
- Встановленням металевих ґрат у віконних прольотах.

Перший метод полягає використанні спеціальних видів скла замість стандартного скла. Це може бути напівзагартоване, загартоване або багатошарове скло, яке володіє високою стійкістю до ударів та зламу. Також існує скло з металевими проводами між його шарами, які використовуються для підключення до електроконтактних датчиків безпеки. Для зміцнення скла також використовуються захисні пластмасові плівки, які приклеюються до зовнішньої або внутрішньої поверхні вікон. Ці захисні плівки можуть бути двох типів:

- Безпечні (безосколкові), які мають високу міцність;
- Протипожежні, які можуть утримувати поширення вогню до 40 хвилин.

На вікна будівель, які можуть бути потенційним місцем доступу зловмисника до приміщення зі значною інформацією, рекомендується встановлювати ґрати. Особливо це стосується вікон на перших, других або останніх поверхах будівлі, а

також вікон біля зовнішніх сходів або великих дерев. Для захисту віконних прорізів застосовуються два типи решіток:

- Безкаркасні металеві решітки, які вбираються безпосередньо в стіну;
- Каркасні решітки, які мають прути, що прикріплюються до металевої рами та стіни.

Металеві шафи, сейфи та сховища є дуже надійними засобами захисту документів, матеріалів, магнітних та фотоносіїв і навіть технічних засобів: ПЕОМ, калькуляторів, принтерів, ксероксів тощо.

Надійність металевих шаф залежить від міцності матеріалу і надійності замка. Зазвичай вони використовуються для зберігання документів і цінностей низького рівня конфіденційності. Але існують спеціальні металеві шафи, призначені для зберігання ПЕОМ та іншої цінної техніки. Такі шафи оснащуються подвійною системою замикання: ключовим замком та комбінованим замком з трьох-п'ятизначним кодом. Ці шафи надійні і стійкі до вторгнень, що робить їх ефективними проти промислового шпигунства.

Сейфи і сховища, так само як і спеціальні металеві шафи, використовуються для зберігання особливо цінних документів, носіїв інформації, технічних пристроїв і значних сум грошей.

Сейфи - це двостінні металеві шафи з важким наповненням простору між стінками, які можуть бути виготовлені з армованого бетону, композитних матеріалів або багатошарових заповнювачів з різних матеріалів.

Сховища є стійкими до зламу та високих температур конструкціями, з площею основи внутрішнього простору більше двох квадратних метрів. Залежно від конструкції, їх можна класифікувати як монолітні, збірні або збірно-монолітні.

Розподіл об'єкта на зони безпеки є важливим елементом фізичного захисту. Планування будівель, приміщень та об'єктів з урахуванням цих зон дозволяє оцінити значення різних частин об'єкта з точки зору потенційної шкоди від різних видів загроз. Типові зони безпеки включають:

1) Територія об'єкта, обмежена парканом або умовним зовнішнім кордоном.

2) Будівля, розташована на території.

3) Коридор або його частини.

4) Приміщення (службові кабінети, кімнати, зали, технічні приміщення, склади тощо).

5) Шафи, сейфи, сховища.

Зони безпеки повинні бути розташовані послідовно на об'єкті, починаючи від забору навколо території й до сховищ цінностей, утворюючи ланцюг перешкод (рубежів), які чергуються один за одним. Основу планування та обладнання зон безпеки становить принцип рівномірного розподілу меж між ними, а загальна міцність зон безпеки вимірюється найменшою з них.

Рубежі захисту створюються як на межах зони, так і усередині неї. Оптимальне розташування зон безпеки та ефективного технічного обладнання для виявлення, відображення та усунення наслідків незаконних дій є ключовими елементами концепції інженерно-технічного захисту територій та приміщень об'єкта.

Контроль та управління доступом до зон, будівель та приміщень, що підлягають захисту, здійснюється за допомогою систем контролю та управління доступом (СКУД).

1.3. Класифікація об'єктів, що охороняються

Існують різні типи об'єктів залежно від рівня їх фізичного захисту та контролю доступу. Нижче наведені переклади різних типів об'єктів, що відрізняються за заходами безпеки:

- Відкриті об'єкти без обмежень: це об'єкти, до яких можуть мати доступ персонал та відвідувачі без будь-яких перешкод чи контролю.
- Об'єкти з простими обмеженнями: це об'єкти, які мають прості пасивні перешкоди або огорожі, які не охороняються (наприклад, паркани, стіни, грати тощо).
- Об'єкти з контрольованими огорожами: це об'єкти, які мають охоронювані огорожі та контролюються охоронними службами з постовими нарядами, патрульними службами та співробітниками пропускної системи.

- Об'єкти з підвищеним режимом охорони: це об'єкти, де доступ контролюється спеціально підготовленими охоронцями, розташованими на території та периферії. Вони використовують складні інтегровані технічні системи для санкціонування доступу, відеоспостереження та охоронно-пожежної сигналізації, які об'єднані в єдиний комплекс, що управляється комп'ютером і контролюється з центрального пульта охорони.

Після проведення аналізу української та зарубіжної статистики щодо недозволеного проникнення в комерційні структури (офіси, виробничі та складські приміщення), були отримані наступні висновки щодо ефективності різних систем безпеки:

- Для об'єктів першої категорії спостерігається до 50% випадків недозволеного проникнення від загальної кількості спроб.
- Для об'єктів другої категорії цей показник становить близько 25%.
- Для об'єктів третьої категорії цей показник становить близько 20%.
- Для об'єктів четвертої категорії цей показник менше 5%.

(ДСТУ 78.11.001-98 "Укріпленість об'єктів, які охороняються за допомогою пультів централізованого спостереження Державної служби охорони", коментарі)

В залежності від значущості, типу та концентрації матеріальних, історичних, культурних та інших цінностей, які зберігаються на об'єктах і в приміщеннях, ці об'єкти та приміщення розподіляються на три категорії (А, Б, В).

1.Об'єкти категорії "А":

- об’єкти життєзабезпечення населених пунктів; би)фабрики і центральні сховища дензнаков і цінних паперів;
- об’єкти Державного комітету з телебачення і радіомовлення; грам)государственные центральні статистичні управління; д)хранилища державних архівів;
- особенно важливі приміщення, де зберігаються:

- грошові кошти, незалежно від дозволеного залишку зберігання (поштові відділення і вузли зв'язку, виплатні каси підприємств, організацій, установ, головні об'єднані каси торгових підприємств, обмінні пункти валюти і ін.);
- зброя, боєприпаси (стрілецькі тири, кімнати зберігання зброї підприємств і учереж- дений, стрілецькі стенди, магазини по реалізації мисливської і спортивної зброї, майстерні по ремонту зброї і ін.);
- наркотичні і психотропні речовини, прекурсори, отрути (бази аптекоуправлений, аптеки, склади мобрезерва, наукові, медичні і інші установи, в практиці яких використовуються ці речовини);
- дорогоцінні метали і камені, ювелірні вироби з них (ювелірні заводи і майстерні, магазини, ломбарди, бази, склади, сховища підприємств, установ і організацій, які використовують в своїй діяльності дорогоцінні метали і камені, пункти закупівлі дорогоцінних металів і каменів і ін.);
- історичні і культурні цінності державного значення (музеї, картинні галереї, фондохранилища музеїв, наукові бібліотеки і ін.);
- вибухові і радіоактивні речовини і матеріали;
- бази і склади із зберіганням цінностей на суму понад 100 тисяч мінімальних зарплат; е)другие об'єкти державного значення.

2. Об'єкти і приміщення категорії "Б" (підприємства, магазини, бази, сховища і ін.),де зберігаються:

а)комп’ютерна техніка

б)малогабаритна і дефіцитна оргтехніка;

в)відео- і аудіотехніка, яка має попит;

г)кіно-, фототехніка;

д)натуральні і штучні і вироби з них;

д)кожа натуральна і вироби з неї;

е)автомобілі і запасні частини до них;

е)промислові і продовольчі товари повсякденного попиту;

ж)технологічне і господарське устаткування;

з)технична і конструкторська документація;

й) інвентар, напівфабрикати і др.;

і) інші цінні товари.

3. Об'єкту і приміщення категорії "В":

- особисте майно громадян (квартири, садиби громадян, гаражі, дачі, автомобільні стоянки і ін.)

1.4. Класифікація систем охоронної сигналізації

На ринку існує широкий вибір технічних засобів для систем охоронної сигналізації. Багато систем сигналізації мають спільні ознаки, такі як:

а) Чутливий елемент або сенсор, який реагує на зміну фізичного параметра і перетворює його на електричний сигнал або зміну сигналу.

б) Аналізатор сигналу, який виявляє представницький параметр, що містить інформацію про зміну параметра, порівнює його з граничним значенням або еталоном і, якщо поріг перевищений, генерує сигнал тривоги.

Сенсори є ключовими елементами в системі сигналізації, і вони базуються на різних фізичних принципах дії. В залежності від принципу дії, використовуваного ефекту, параметра, форми та інших характеристик, сенсори можуть бути класифіковані в різні системи виявлення. Деякі з них вимагають спеціальних конструкцій, які дублюють огорожу по всьому периметру, наприклад, ємнісні, натяжні системи або "електричні стіни". Інші чутливі елементи можуть бути безпосередньо встановлені на наявних огорожах без необхідності значних будівельних робіт.

Існує значний інтерес до використання заходів захисту для об'єктів, особливо останніх. Залежно від характеру та значимості об'єкта, різні заходи передбачаються для захисту його периметра. Периметр об'єкта визначається як лінія, що обмежує територію, і він часто співпадає з огорожею навколо об'єкта. Він може бути

позначений також межами, валами, ровами, канавами, зеленими насадженнями або попереджувальними знаками. Лінія периметра може бути також відзначена на плані, у будівельній документації або в правових документах, навіть якщо фізично не виділяється на місцевості.

Головна мета охорони об'єкта полягає в унеможливленні несанкціонованого проникнення окремих осіб або груп на його територію. Охорона починається з охорони периметра. Іншим аспектом охорони є забезпечення вільного проходу або проїзду на територію об'єкта для тих, кому це дозволено. Очевидно, що охорона периметра завжди супроводжується контролем і керуванням доступом. Рівень захисту об'єкта повинен відповідати загрозам, що можуть виникнути внаслідок несанкціонованого проникнення. Загроза стає очевидною, коли потенційний порушник намагається проникнути на об'єкт. Охоронна сигналізація периметра використовується для виявлення цього моменту. Захист периметра садової ділянки зазвичай зводиться до встановлення дерев'яного забору або металевої сітки "рабиця".

Такі об'єкти, як дачні або котеджні селища, часто оточують огорожами та залучають сторожів або охоронців для забезпечення безпеки. Ексклюзивні котеджі та престижні пансіонати використовують служби охорони та технічні засоби для забезпечення безпеки. Промислові підприємства, заводи, склади, сховища, аеропорти також застосовують інженерні та технічні засоби захисту периметра, утримуючи служби безпеки.

Значно серйозніші заходи організовують для захисту небезпечних виробництв, секретних об'єктів, військових установ та в'язниць. На таких об'єктах передбачається декілька рівнів захисту периметра, які включають комбіновані інженерні споруди, охоронну сигналізацію та спеціальні заходи безпеки. Складність системи охоронної сигналізації периметра повинна відповідати рівню загроз. При виборі такої системи необхідно враховувати як інженерні заходи для зміцнення периметра, так і загальну стратегію охорони об'єкта.

Один з ефективних методів збору необхідної інформації - це проведення технологічного обстеження периметра об'єкта. Це дослідження слід проводити перед будь-якими іншими проектними роботами. Під час обстеження важливо оцінити можливі шляхи незаконного проникнення на об'єкт і визначити види та ступінь перешкод, які можуть виникнути при таких спробах. Технологія захисту периметра об'єкта завжди пов'язана з двома процесами: ідентифікацією відвідувачів (включаючи небажаних) та контролем їх проходження (або непроходження) на чи з об'єкта. Для першого процесу використовуються технічні засоби телевізійного спостереження, а для другого - засоби контролю та керування доступом.

Давайте розглянемо два типові сценарії.

У першому сценарії відвідувач підходить до контрольно-пропускного пункту (хвіртки, ворота) та натискає кнопку виклику. Це спричиняє сигнал до чергового оператора і активацію системи телевізійного спостереження. Телевізійний сигнал від камери, спрямованої на відвідувача, транслюється на головний екран або відображається в повноекранному вікні відеомонітора, і запускається програма розпізнавання образів. Ця програма порівнює ознаки образу з камери з ознаками образів, які зберігаються в архіві телевізійної системи. Якщо в архіві знайдено образ з достатньою кількістю ознак, які співпадають з ознаками відвідувача, фотографія суб'єкта з архіву разом з короткими відомостями про нього виводиться на другий екран або в окреме вікно відеомонітора. Це дає черговому оператору служби безпеки достатньо інформації для візуальної ідентифікації двох образів. Також система автоматично починає записувати зображення з відеокамери на відеонакопичувач у реальному часі.

У разі, якщо автоматичне розпізнавання образу невдається, на екрані з'являється повідомлення "Образ не знайдено".

Після ідентифікації відвідувача, оператор приймає рішення щодо пропуску або непропуску особи. У разі прийняття рішення про пропуск, оператор звертається до системи керування доступом. Спочатку він активує реле обходу воріт або хвіртки, відключаючи їх від зони охорони периметра. Потім натискає кнопку

дозволу проходу або проїзду, що призводить до розблокування замка і включення привода відчинення воріт або хвіртки. Відбувається відкриття воріт або хвіртки для пропуску відвідувача.

Після контрольованого пропуску з використанням оповіщувача присутності, ворота або хвіртка автоматично закриваються. Після проходу відвідувача, черговий оператор відключає блокування воріт або хвіртки, і вони знову включаються в зону охорони периметра.

У випадку, коли рішення приймається щодо непропуску відвідувача, оператор діє відповідно до інструкцій, встановлених на об'єкті. Усі дії відвідувача записуються в режимі реального часу в накопичувач. Також реєструються всі зміни стану обладнання та команди оператора. Цей електронний запис зберігається в архіві і може використовуватися для аналізу минулих подій.

Другий сценарій випадає, коли порушник спробує незаконно проникнути на об'єкт через огорожу. У такому випадку система охоронної сигналізації периметра сприймає цю спробу і активує сигнал тривоги, який відображається на пульті оператора.

Цей сигнал спричиняє підключення звукового монітора до звукового каналу зони, яка була порушена, і звуковий монітор відтворює звуки вібрацій, спричинених порушником. Крім того, сигнал тривоги ініціює перемикання зображення від відеокамери, що моніторить порушену зону, на головний екран або в повноекранне вікно відеомонітора, а також записує подію, що фіксується камерою, в реальному часі на відеонакопичувачі.

Оператор отримує можливість бачити та чути подію, що відбувається в порушеній зоні охоронного периметру. Після оцінки рівня небезпеки події оператор приймає рішення та вживає заходів, передбачених інструкцією, яка була встановлена на об'єкті. Електронний запис події, що містить зображення, звук, інформацію про стан обладнання, його зміни, включаючи команди оператора, зберігається в архіві. Цей запис може бути використаний для подальшого аналізу події.

Таким чином, система охоронної сигналізації периметру поєднується з системою відеоспостереження та системою керування доступом. Для такого поєднання система охоронної сигналізації має додаткові виходи для передачі команд та сигнальні виходи для взаємодії з зовнішніми пристроями та системами. В багатьох випадках передбачаються додаткові входи для отримання команд від зовнішніх пристроїв та систем. Наприклад, від детектора руху системи відеоспостереження може надходити сигнал, що ініціює підключення звукового монітора до звукового каналу тієї зони, в якій виявлено потенційного порушника. У цьому випадку оператор має можливість контролювати зону на слух ще до початку спроби вторгнення. Система охоронної сигналізації периметру може бути підключена до системи оповіщення, системи відображення та інших зовнішніх систем.

У таких випадках, при спробі вторгнення, порушник може бути попереджений голосовим повідомленням про те, що він вторгся в охоронювану зону, і при цьому освітлюється прожектором. У багатьох випадках цього виявляється достатньо, щоб порушник припинив подальші спроби вторгнення. Розташування точок підключення обладнання та порядок їх взаємодії визначаються на етапі проектування системи. Перед проектуванням системи важливо провести технологічний аналіз, що враховує можливі дії оператора служби охорони, після чого виконується системне та схемне проектування.

РОЗДІЛ 2 ЗАГАЛЬНІ ВІДОМОСТІ ПРО ІНТЕГРОВАНУ ОХРОННУ СИСТЕМУ ДУНАЙ

2.1. Модулі підключення охоронної системи Дунай

Модуль живлення виконаний за схемою імпульсного перетворювача з максимальним

вихідним струмом на навантаженні 0,5 А. Акумулятор підключений в буфер до вихідних контактів через вузол обмеження струму заряду.

При відключенні напруги електромережі включається індикатор ПТ/РА з періодом 500 мс шпаруватість 2, а ППК перемикається на роботу від акумулятора. При відновленні напруги в мережі 220 В, ППК формує повідомлення МЕРЕЖА 220 В НОРМІ і включає індикатор ПТ/РА з постійним світінням.

При розряді акумулятора до (10,8±0,25) ППК формує повідомлення АКУМУЛЯТОР РОЗРАЖЕНИЙ і включає індикатор ПТ/РА з періодом 250 мс шпаруватість 2. При цьому біпер видає подвійний короткий сигнал раз на дві секунди.

При розряді акумулятора нижче (10,0±0,6) і відсутності напруги електромережі модуль живлення автоматично вимикається.

Модуль живлення включається автоматично при підключенні до нього акумулятора з напругою на клемах не менше 12 В та відсутності напруги в електромережі.

Під час заряджання акумулятора напруга на контактах «12V» модуля збільшується в міру заряду акумулятора.

Ланцюг підключення клем акумулятора до модуля живлення захищений вставкою плавкою FU1 1А, що знаходиться на платі модуля живлення.

Ланцюг електроживлення від електромережі 220 захищена вставкою плавкою FU1 0,25А, яка знаходиться в блоці м

Режими роботи ППК

ППК, незалежно від виду застосування, може перебувати в одному із станів:

РОБОТА;

ПРОГРАМУВАННЯ;

СЕРВІСНІ РОБОТИ.

У стані РОБОТА виконуються режими:

- черговий;
- перегляд стану груп;
- переглядстану шлейфів групи;
- зміна охоронного стану групи (взяття/зняття під охорону);
- перегляд пам'яті тривог;

У черговому режимі ППК перебуває завжди за відсутності будь-яких сформованих повідомлень передачі на зовнішній пристрій чи ПЦН.

У черговому режимі може бути виконано переведення ППК в один із перерахованих вище режимів роботи. У цьому режимі:

- індикатор жовтого кольору «ПТ/РА»:
- включений – за наявності напруги електроживлення від мережі 220 В;
- блимає з періодом 500 мс шпаруватість 2 при відключенні напруги мережі;
- блимає з періодом 250 мс шпаруватість 2 при відсутності напруги мережі та розряді акумулятора до 10,8 В;
- вимкнено – за відсутності напруги мережі та розряду акумулятора нижче 10 В.

індикатор «ПІДТВ ВЗЯТТЯ» червоного кольору:

- безперервно світиться, якщо приміщення (група шлейфів) взято під охорону та отримано підтвердження від ПЦН про взяття під охорону;
- блимає з періодом 250 мс шпаруватість 2 при фіксації тривоги по шлейфу і запису її на згадку про тривоги;
- блимає з періодом 500 мс шпаруватість 2 при блокуванні взяття під охорону, якщо ППК охороняє лише одну групу;
- відображає коди параметрів у режимі програмування;
- не світиться, якщо немає записів у пам'яті тривог або група (групи) знята з охорони.

У режимі перегляду стану груп може бути виконано перегляд числа груп, що охороняються, і стану кожної групи. Для переходу в цей режим із чергового режиму необхідно з клавіатури ввести послідовність 0 #, при цьому прийом послідовності біпер підтвердить двома короткими сигналами.

У цьому режимі індикатори "1" - "4" відображають стан груп, причому, індикатор "1" відображає стан групи 1, "2" - групи 2 і т.д. Увімкнені або блимають лише світлодіоди груп, введених у конфігурацію ППК під час програмування.

Індикатори блимають у форматах:

- з періодом 250 мс при шпару 2 при тривозі по групі, взятій під охорону;
- з періодом 500 мс при шпару 2 при блокуванні взяття групи під охорону.
- Індикатори вимкнені для відсутніх та знятих з охорони груп.

Для виходу з режиму та повернення до чергового режиму необхідно натиснути клавішу.

У режимі перегляду стану шлейфів групи може бути виконано перегляд на індикаторах "1" - "4" стану шлейфів групи. Для переходу в цей режим необхідно в черговому режимі або перегляду стану груп з клавіатури ввести послідовність

1 номер групи #.

Якщо група із запитуваним номером є у конфігурації ППК, біпер підтвердить двома короткими сигналами прийом запиту. При запиті неіснуючої групи можливість перегляду відкинеться, про що біпер повідомить одним коротким і одним довгим сигналами.

У цьому режимі індикатори можуть відображати такі стани шлейфів:

- індикатор включений – шлейф перебуває у стані НОРМА;
- індикатор вимкнений, коли група під охороною - шлейф не належить групі, що проглядається;
- індикатор вимкнений, коли група знята з охорони - шлейф або не належить групі, або його опір вище за норму;
- індикатор блимає з періодом 250 мс при шпару 2 - шлейф знаходиться в стані ТРИВОГА;

- індикатор блимає з періодом 1 с при шпару 8 (короткочасно спалахує) – опір шлейфу менше норми.

Біпер генерує подвійний короткий сигнал раз на секунду при тривозі протягом 1 хвилини або до натискання кнопки 1#2 (крім тривожного шлейфу).

У режимі перегляду стану шлейфів групи виконується зміна стану охорони групи (взяття/зняття під охорону). Для цього в цьому режимі необхідно ввести: код доступу користувача 1#2 (у заводських установках код «789» за промовчанням для користувача №1). Порядок призначення, зміни, видалення кодів користувачів наведено в 1.8 цього посібника.

Правильне введення біпер підтверджує двома короткими сигналами, а обрана група змінить свій стан на протилежне. Наприклад, якщо групу взято під охорону – буде знято (вимкнеться індикатор ВЗЯТО та ввімкнеться індикатор ЗНЯТО) або навпаки, якщо всі шлейфи в нормі, або після закінчення часу затримки на вхід/вихід. При неправильному введенні коду доступу користувача біпер просигналить одним коротким і одним довгим сигналами і стан охорони групи не зміниться.

При централізованій охороні з автоматизованою тактикою діє зняття примусової групи, коли введено код доступу користувача на одиницю, що перевищує запрограмований код.

Для виходу з режиму перегляду стану шлейфів групи та переходу до чергового режиму ввести 1 2 3.

У режимі перегляду пам'яті тривог може бути виконаний перегляд послідовності порушення шлейфів групи, що охороняється.

Для переходу в цей режим з перегляду стану шлейфів групи необхідно ввести послідовність 9 #, при цьому прийом послідовності біпер підтвердить двома короткими сигналами.

У цьому режимі індикатори «1» – «4» можуть відображати:

- індикатор вимкнено – немає тривоги шлейфу;

- індикатор блимає з періодом 250 мс при шпару 2 - шлейф був порушений першим;індикатор блимає з періодом 500 мс при шпару 2 - шлейф був порушений другим;
- індикатор блимає з періодом 1 с при шпару 2 - шлейф був порушений третім;
- індикатор світиться безперервно – шлейф було порушено четвертим. Пам'ять тривог стирається після чергового взяття групи під охорону.

Для виходу з режиму та переходу в режим відтворення стану шлейфів необхідно ввести 1 2 3.

Стан ПРОГРАМУВАННЯ.

Стан програмування або інакше – режим програмування призначений зміни конфігурації.

Для переходу в цей режим необхідно в черговому режимі ввести послідовність □код адміністратора 1 2 #3 (код «123» за умовчанням, порядок зміни коду наведено в 1.8 цього посібника).

Правильний введення біпер підтвердить чотирма короткими сигналами і одночасно вмикаються індикатори «ВЗЯТО» та «ЗНЯТО».

Для виходу з режиму програмування необхідно ввести □□□, при цьому виконається скидання ППК та його налаштування на введену конфігурацію.

Процедуру входу/виходу в режим програмування можна використовувати для скидання ППК.

Опитування стану ППК ініціюється ПЦН. ППК, розпізнавши команду опитування, формує повідомлення про стан шлейфів, груп та ППК на даний момент часу та передає їх на ПЦН.

Роботою керуючого виходу «UK» та вихідним реле керує контролер відповідно до встановлених при програмуванні ППК реакцій.

Взяття або зняття з охорони може також виконуватися за допомогою клавіатури типу «Дунай-КА», підключеної до 4-го шлейфа ППК, але при цьому не можна взяти/зняти з основної клавіатури ППК.

Налаштування ППК на режим роботи з клавіатурою типу «Дунай-КА» виконується в режимі програмування за допомогою функції 3, код параметра 6 для

виконання «Дунай-4.1» та «Дунай-4.2», як зазначено в 1.8.2.4 або за допомогою функції 2, код параметра 6 для виконання "Дунай-1", як зазначено в 1.8.3.3 цього посібника.

2.2. Огляд інтегрованих систем і комплексів для охоронної системи Дунай

1 ППК «Дунай-4», призначені для прийому сповіщень по шлейфах сигналізації від сповіщувачів або від інших ППК, у тому числі від ППК типу «Дунай», «ВБД4», «ВБД6», перетворення сигналів, видачі сповіщень для безпосереднього сприйняття людиною та (або) подальшої передачі повідомлень на пульт централізованого спостереження та (або) включення зовнішнього оповіщувача.

2 ППК забезпечує автономне чи централізоване застосування. Автономне застосування використовується охорони локальних об'єктів без передачі сповіщень про тривозі на пульт централізованого спостереження (ПЦН). Централізоване застосування забезпечує роботу ППК у складі систем тривожної сигналізації з використанням каналів зв'язку передачі на ПЦН сповіщень про тривозі.

3 ППК «Дунай-4» виготовляються у трьох виконаннях: «Дунай-4.1», «Дунай-4.2» та «Дунай-1».

Таблиця 2.1 - Варіанти виконання ППК за способом застосування

Вид застосування ППК	Виконання ППК		
	Дунай-	Дунай-	Дунай-
1 Автономне застосування для охорони об'єктів:			
- без передачі повідомлень на ПЦН	+	+	+
- з передачею повідомлень на мобільний телефон у форматі SMS повідомлень мережі GSM 900/1800	-	-	+

Продовження таблиці 2.1

- з передачею повідомлень на ПЦН зайнятою телефонною лінією міської телефонної мережі (ГТС)	-	+	-
- з передачею повідомлень на ПЦН через мережу стільникового радіозв'язку стандарту GSM900/1800 в режимі GPRS і в режимі передачі SMS	-	-	+
3 Централізоване застосування з ручною тактикою охорони у складі СПДІ «Дунай-XXI», СПІ "Центр", "Нева", "Атлас"	-	+	-

4 Кліматичне виконання ППК за умовами розміщення на об'єкті задовольняють згідно з ГОСТ 15150 групи УХЛ, категорії виробу 3.1, а саме:

5- Кліматичне виконання ППК за умовами розміщення на об'єкті задовольняють згідно з ГОСТ 15150 групи УХЛ, категорії виробу 3.1, а саме:

- ППК можуть експлуатуватися в закритих приміщеннях, що не опалюються з природною вентиляцією, з регульованим кліматом в діапазоні робочих температур навколишнього середовища від мінус 10 до плюс 40°С;
- ППК стійкі до впливу підвищеної відносної вологості середовища не більше 93% за температури навколишнього середовища не вище плюс 30°С;
- ППК, упаковані в транспортну тару, стійкі до впливу температури навколишнього середовища від мінус 25 до плюс 55°З відносної вологості повітря 95% при температурі не вище плюс 35°С.

ППК забезпечує показники, наведені у таблиці 2.2

Таблиця 2.2 - Показники ППА

Параметр	Виконання ППК		
	Дунай-	Дунай-	Дунай-
1 Інформаційна ємність (кількість шлейфів)	4		
2 Інформативність (перелік повідомлень наведено в таблиці 3), од., не менше	12		
3 Реакція на розрив шлейфу: - формується повідомлення у разі порушення шлейфу тривалістю, мс, і більше;	70		
- відсутня при порушенні шлейфу тривалістю, мс, і менше	50		
4 Кількість програмованих груп шлейфів (мінімальна кількість шлейфів у групі – 1, максимальне - 4), не більше	від однієї до чотирьох		
5 Кількість користувачів (ключів доступу) для доступу до управління взяттям/зняттям груп (розмір Pin-коду – до 4 цифр)	24		
6 Наявність пам'яті тривог	+	+	+
7 Тривалість повідомлення про тривогу, не менш,	-	2	-
8 Параметри шлейфу: - опір витоку між проводами та кожним проводом та землею, не менше: для охоронного шлейфу, ком для пожежного шлейфу, ком - опір виносного резистора, кОм	20 50 2,7		
9 Напруга на контактах у точках підключення шлейфу (при розімкнутому шлейфі), В, не менше	10		
10 Постійний струм у шлейфі з урахуванням опору витоку за п. 8, Ма	від 1,1 до 2,5		

Продовження таблиці 2.2

11 Кількість вихідних реле (контакт, що перемикається, комутована потужність не менше 6 Вт), шт	1	1	-
12 Наявність керованого виходу «UK» типу «відкритий колектор», що забезпечує комутований струм не більше 0,3 А при напрузі постійного струму не більше 14 Ст.	+	+	+
13 Автономне застосування ППК для охорони об'єктів без передачі сповіщень на ПЦН	+	+	+
14 Централізоване застосування ППК з автоматизованої тактики охорони у складі СПДІ «Дунай-XXI», «Дунай-ПРО» з передачею повідомлень на ПЦН зайнятою телефонною лінією ГТС	-	+	-
15 Централізоване застосування з ручною тактикою охорони у складі СПДІ «Дунай-XXI», СПІ "Центр", "Нева", "Атлас"	-	+	-
16 Централізоване застосування ППК з автоматизованої тактики охорони у складі СПДІ "Дунай-XXI", "Дунай-ПРО" з передачею повідомлень на ПЦН по мережі стільникового радіозв'язку стандарту GSM900/1800 в режимі GPRS і в режимі передачі SMS	-	-	+
17 Автономне застосування ППК з передачею повідомлень на мобільний телефон у форматі SMS повідомлень мережі GSM 900/1800	-	-	+
18 Час технічної готовності, не більше, з	60		

Таблиця 2.3 - Перелік повідомлень, що формуються ППК

Перелік повідомлень	Умови формування	Стан індикатора
1	2	3
1 Тривожні повідомлення: - Тривога (обрив шлейфу)	При збільшенні повного опору шлейфу більше 3,51 кОм, при цьому приміщення (група) має бути взято під охорону.	Індикатор стану шлейфу блимає з періодом 250 мс (шпаруватість 2) довідновлення шлейфу в норму, але не менше 1 хвилини. Для виконання

		"Дунай-4.2" повідомлення повинно передаватися на ПЦН, для "Дунай-1" - на ПЦН або мобільний телефон1).
- Тривога (КЗ шлейфу)	При зменшенні повного опору шлейфу менше 1,89 ком, при цьому приміщення (група) має бути «взято під охорону».	Те саме
- акумулятор розряджений	При зникненні напруги електромережі та зниженні напруги на клемах акумулятора до (10,8±0,25).	Індикатор “ПТ/РА” блимає з періодом 0,25 с (шпарування 2). Для виконання «Дунай-4.2» повідомлення має передаватися на ПЦН, для «Дунай-1» – на ПЦН чи мобільний телефон2).
- Відкрита дверця	При відкритті дверцята корпусу ППК.	Індикатор не передбачено. В виконанні «Дунай-4.1» включається біпер на якийсь час до закриття дверцят. Для виконання «Дунай-4.2» повідомлення має передаватисяна ПЦН, для «Дунай-1» - на ПЦН чи мобільний телефон2).
Зняття примусово	При введенні коду користувача, у якому значення останньої цифри коду на одиницю більше.	Індикатор “ЗНЯТО” вмикається, “ВЗЯТО” - вимикається. Для виконання «Дунай-4.2» повідомлення має передаватисяна ПЦН, для «Дунай-1» - на ПЦН чи мобільний телефон2).

Продовження таблиці 2.3

2 Заявні повідомлення: - Відсутність мережі 220В	При відключеннінапруги електромережі 220 В ланцюга електроживлення ППК.	Індикатор “ПТ/РА” блимає з періодом 0,5 с (швидкість 2) до вмикання напруги мережі. Для виконання "Дунай-4.2" повідомлення повинно передаватися на ПЦН, для "Дунай-1" - на ПЦН або мобільний телефон2).
- Обрив шлейфу	При збільшенні повного опору шлейфу (опір виносного резистора, проводу шлейфу та ланцюгів витоку) більше 3,51кОм, при цьому приміщення (група) має бути «знято» з охорони (з урахуванням виносного резистора, проводу шлейфу та ланцюгів витоку). При зачиненні дверцят корпусу ППК	Індикатор стану шлейфу вимкнено до відновлення шлейфу в норму або переходу шлейфу до іншого стану. Для виконання «Дунай-4.2» та «Дунай-1» повідомлення має передаватися на ПЦН під час опитування стану ППК2).
-Закрита дверця		Індикатор не передбачено. Для виконання «Дунай-4.1» вмикається переривчастий сигнал біпера до закриття дверцят. Для виконання "Дунай-4.2" повідомлення повинно передаватися на ПЦН, для "Дунай-1" - на ПЦН або мобільний тел.
- Шлейф невиправлений (опір шлейфу менший за норму)	При зменшенні повного опору шлейфу менше 1,89 кОм, приміщення (група) має бути «знято з охорони».	

ППК складається з функціонального блоку «Дунай-4» відповідного виконання, модуля живлення «Дунай-ІС05» та резервного джерела (акумулятора 12 2,4 Ач). У виконання ППК додатково встановлено:

- в "Дунай-4.2": вузол сполучення з телефонною лінією на модулі "Дунай-4СМ2" функціонального блоку;
- у «Дунай-1»: радіотермінал прийому/передачі повідомлень (повідомлень) у форматі SMS мережі
- GSM 900/1800 на ПЦН або мобільний телефон.

Індикатори та клавіатура.

Світлодіодні індикатори, розміщені на передній панелі функціонального блоку ППК, відображають:

- «1»–«4»- стани шлейфів;
- «Взято»- приміщення (група) під охороною;
- «ЗНЯТО» - приміщення (група) знято (знято) з охорони;
- «ПІДТВ ВЗЯТТЯ»- підтвердження користувачеві про взяття під охорону приміщення (групи);
- «ПТ/РА»- наявність напруги мережі чи розряд акумулятора.

У виконанні Дунай-1 індикатори можуть відображати стан радіотерміналу при включенні функції Стан терміналу (див. п. ….).

Клавіатура забезпечує виконання режимів:

- черговий (клавіатура не активна);
- перегляд стану груп. Поняття «стан групи» шлейфів та «стан приміщень» еквівалентні;
- перегляд пам'яті тривог;
- перегляд стану шлейфів груп (приміщень);
- програмування;
- сервісний;
- перегляд стану радіотерміналу;
- тест перевірки справності індикаторів.
- Під час програмування або вибору сервісного режиму ППК не виконує функції охорони

У централізованому застосуванні виконання ППК «Дунай-4.2» забезпечує функціонування:

- у складі СПДІ «Дунай-XXI», при цьому передача сповіщень на ПЦН забезпечується при підключенні ППК до ретрансляторів «Дунай-Р1000» або «Дунай-Р»;
- у складі КІСЦН «Дунай» або АІУС «Каштан», при цьому передача сповіщень на ПЦН забезпечується через ретранслятор «Дунай-Р» або «Каштан» відповідно.
- ППК забезпечує контроль несанкціонованого доступу до корпусу. В автономному застосуванні при відкриванні дверцят корпусу ППК реле включається на 1 хвилину (для виконань «Дунай-4.1», «Дунай-4.2»),
- якщо до цього воно не було включено, біпер видає сигнал тривалістю 0,5 разів на секунду до закриття дверцята.

У централізованому застосуванні при відкритті дверцята корпусу ППК на ПЦН передається повідомлення ДВЕРЦЯ ВІДКРИТА, при закритті – ДВЕРЦЯ ЗАКРИТА. При централізованому застосуванні з ручною тактикою охорони біпер видає сигнал тривалістю 0,5 разів на секунду до закриття дверцят.

ППК забезпечує цілодобове функціонування при електроживленні від мережі змінного струму напругою від 187 до 242 В частотою (50 1) Гц.

ППК забезпечує автоматичне перемикання на електроживлення від резервного джерела (акумулятора) при відключенні напруги мережі та назад без видачі тривожного сповіщення. Напруга акумулятора - від (10,8±0,25) до (13,6±0,2).

Час роботи ППК у нормальних кліматичних умовах від вбудованого, зарядженого до повної ємності, акумулятора напругою 12 В ємністю 2,3 А·ч в «черговому» режимі не менше 12 годин, і ще в режимі «тривога» - не менше чотирьох годин.

ППК забезпечує заряд розрядженого до (10,8±0,25) акумулятора. Час заряду не більше 24 год. ППК обмежує струм заряду лише на рівні (0,2±0,02)А.

ППК забезпечує електроживлення підключених до нього зовнішніх споживачів напругою постійного струму від 10,5 до 13,8 при струмі навантаження не більше 0,35 А і пульсаціях вихідної напруги (подвійна амплітуда) не більше 100 мВ.

При підключенні зовнішнього навантаження зі струмом споживання більше 0,35 А електроживлення навантаження здійснюватиме від додаткового джерела, що має резервний акумулятор.

Споживана ППК потужність від мережі змінного струму при напрузі 242 В в черговому режимі, не більше 9 ВА, режимі «Тривога» не більше 11 ВА.

Споживаний ППК струм від акумулятора за відсутності мережі в черговому режимі не більше 0,2 А, режимі «Тривога» трохи більше 0,25 А.

Габаритні розміри корпусу ППК трохи більше: ширина – 230 мм, висота – 230 мм, глибина – 100 мм.

Габаритні розміри корпусу функціонального блоку при роздільній установці його від корпусу ППК, не більше ширина – 175 мм, висота – 100 мм, глибина – 30 мм.

Маса ППК з акумулятором (без упакування), не більше, 5 кг.

2.3. Принцип роботи охоронної системи Дунай

Щоб наш пристрій комунікував з нами, нам знадобиться відповідний модуль, тобто GSM. Він передаватиме тривожні сигнали, а також через нього здійснюватиметься управління системою. Подібні модулі широко застосовують у платіжних системах, моніторингу станів, охороні та інших сферах, де необхідне використання бездротових мереж. Популярними через якість, ціни та можливості є

GSM модулі, які представлені дев'ятисотою і восьмисотою лінійкою (SIM900 і SIM800). Вони є модулями GPRS, GSM, до того ж дуже бюджетні.

Вони мають дуже маленький розмір корпусу, який містить торцеві контакти, що в свою чергу робить полегшення монтажу. Додамо, що вся ця серія побудована на одній і тій же апаратній та програмній платформі. Вони лише різні у кількості функціональних особливостей. Але не дивлячись на це, всі вони можуть виконувати такі функції як відправка смсок, CSD дзвінки і з'єднання по голосовому каналу. Для подібних модулів створені спеціальні команди AT, які дозволяють налаштовувати роботу модулів. Також ці команди дуже схожі і є замінними, якщо ви одного разу познайомилися з ними, то, перейшовши на інший модуль, у вас не виникне проблем з ними. Наші модулі працюють із протоколами HTTP, а також FTP. Швидкість вивантаження у модуля восьмисотої серії значно більша, ніж у дев'ятисотого. Восьмисотий модуль новий, але все ж таки відмінності з дев'ятисотим є, але вони незначні і містяться в дрібницях. Його можливості розширено, цьому також є факт того, що дев'ятисота серія була знята з виробництва.

Таблиця 2.4 - Характеристики SIM900 та SIM800

Характеристики	SIM900	SIM800
Діапазон GSM, МГц	850, 900, 1800, 1900	850, 900, 1800, 1900
Клас передачі даних GPRS	multi-slot class 10,8	multi-slot class 12
Відповідність стандарту GSM	фази 2/2+	фази 2/2+
Клас потужності	4 (2 Вт в діапазонах 850/900 МГц), 1 (1 Вт у діапазонах 1800/1900 МГц)	4 (2 Вт у діапазонах 850/900 МГц), 1 (1 Вт у діапазонах 1800/1900 МГц)
Маса, г	6.2	3.14

Продовження таблиці 2.4

Аудіокодеки	HR, FR, EFR, AMR, придушення луна	HR, FR, EFR, AMR, придушення луна
Вбудований стек	TCP/IP, UDP/IP	TCP/IP, UDP/IP
Протоколи HTTP та FTP	доступні у додатковій, розширеній прошивці	доступні в базовій прошивці
Декодування DTMF-тонів	доступні в додатковій, розширеній прошивці	доступні в базовій прошивці
Інтерфейси	USB, UART	USB, Bluetooth, PCM, 2*UART
Напруга живлення ,	3.2-4.8	3.4-4.4
Робочий температурний діапазон, °C	від -30 до +80	від -40 до +85

На рисунку 2.1 представлена загальна схема системи адресної охоронної сигналізації "Дунай", розроблена за допомогою програми AutoCAD.

При розробці цієї схеми був використаний комплексний підхід з урахуванням необхідної експлуатаційної надійності, особливо в умовах вологого клімату. Були створені умови для подальшого розвитку системи, з урахуванням можливих модифікацій і змін, які можуть з'явитися в процесі експлуатації.

Запропоноване рішення є результатом аналізу попередніх проектів. Технічне рішення, яке було прийнято, базується на комплексному підході до захисту офісної будівлі.

Для запобігання проникненню в об'єкт передбачено блокування люків за

допомогою сповіщувача СОМК 1-8. Щоб уникнути проникнення через бетон, використовуються ІЧ-сповіщувачі Optex LX-402. Таким чином, зони виявлення максимально охоплюють об'єм шахти.

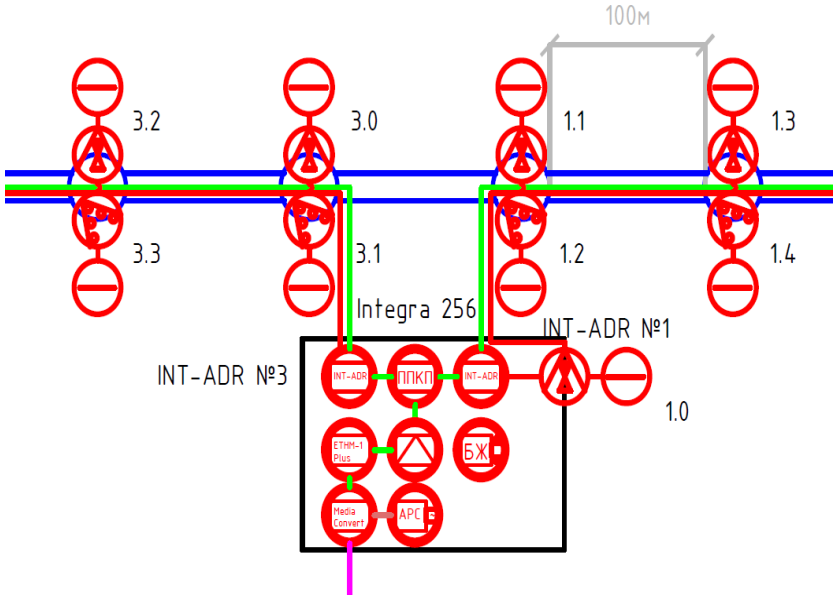

Рисунок 2.1 - Принципова схема адресної охоронної сигналізації

Умовні позначення до рис. 2.1 приведені на рис. 2.2

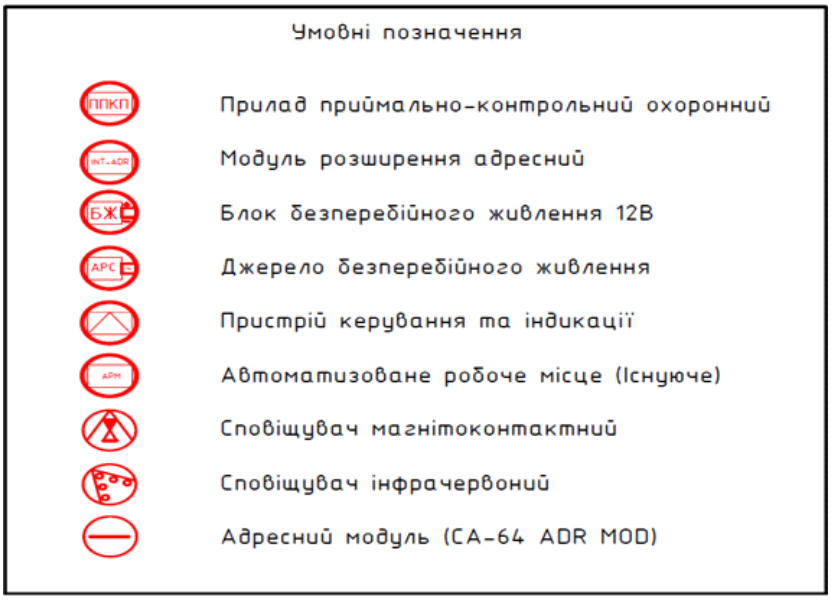

Рисунок 2.2 - Умовні позначення до принципової схеми адресної охоронної сигналізації

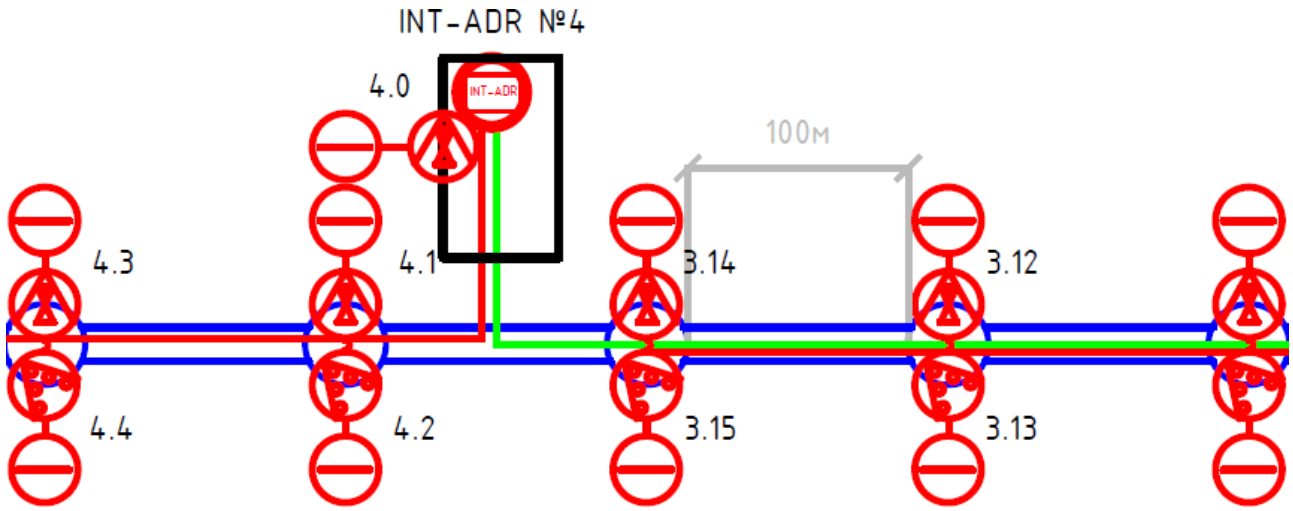

Рисунок 2.3- Принципова схема підключення дальніх модулів та сповіщувачів

Для забезпечення стабільної роботи системи ми плануємо підключити 16 сповіщувачів та 16 адресних модулів СА-64 до одного модуля INT-ADR. Це означає, що з лівої та правої сторони ми зможемо охопити 8 шахт. Щодо двох залишених шахт на кожній стороні, вони будуть підключені до окремого модуля INT-ADR. На рисунку 2.4 показана схема підключення віддалених сповіщувачів.

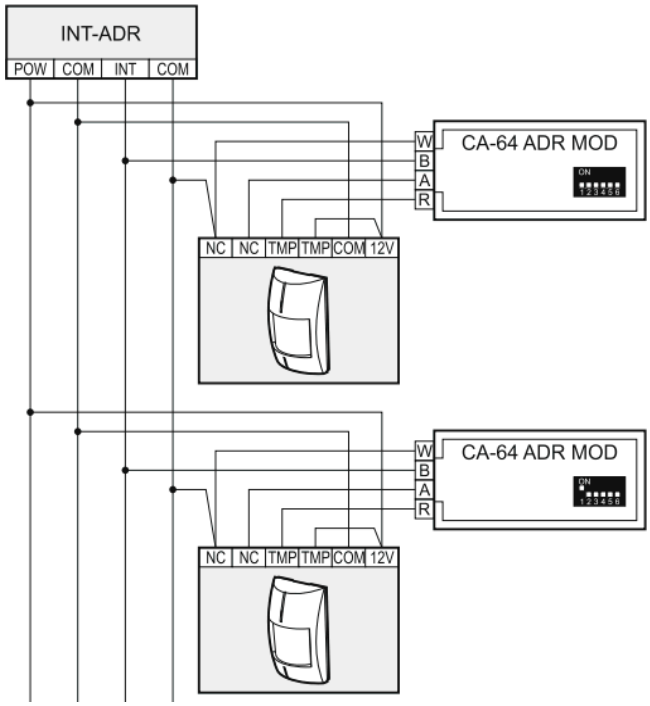

Рисунок 2.4 - Типова схема підключеня сповіщувачів Optex LX-402

Ми використовуємо різні кольори проводів для позначення їх функціональності в системі:

- Білий провід (W) використовується як маса з напругою 0 В.
- Чорний провід (B) є вхідним для передачі даних.
- Синій провід (A) є вхідним, який контролює стан сповіщувача.
- Червоний провід (R) є вхідним для живлення.

Крім того, у нас є такі вихідні та вхідні точки підключення:

- Вихід POW надає постійний струм +12 В DC для живлення адресних модулів CA-64 ADR-MOD та сповіщувачів.
- COM використовується як маса з напругою 0 В.
- Вхід INT використовується для отримання даних від адресних модулів CA-64 ADR-MOD.
- Вхід TMP є тамперним входом, який за замовчуванням замкнутий на масу.
- Вхід CLK є шиною зв'язку для модулів розширення.

Згідно з вимогами виробника продукції марки Satel, максимальна відстань між адресним сповіщувачем і модулем розширення становить 1000 м. У таблиці 2.5 представлені вимоги щодо використання проводів з діаметром жилки 0,5 мм.

Таблиця 2.5 - . Вимоги щодо кількості жил кабеля

Відстань від модуля розширення	Кількість з'єднаних паралельно кабелів
до 200 м	1
200-400 м	2
400-600 м	3
600-1000 м	4

Основуючись на наданих даних, ми розуміємо, що для передачі сигналу на відстань близько 1 кілометра нам потрібно використовувати кабель з 4 жилами діаметром 0,5 мм. Однак, ми можемо замінити цю комбінацію на кабель з 2

жилами діаметром 1 мм. Зважаючи на вищезазначені фактори, ми рекомендуємо використовувати кабель "Алай" КМлВЕеВн 10х1, який має 8 жил діаметром 1 мм, зберігаючи 2 додаткові жилки як резерв.

На рисунку 2.5 показана схема підключення адресного модуля (у даному випадку INT-ADR) до головної плати ППК.

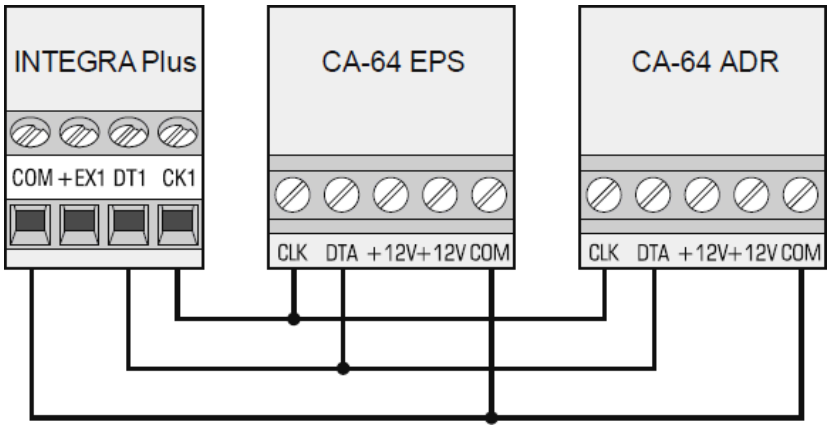

Рисунок 2.5 - Схема підключення адресуючого модуля до головної плати ППК

На (Табл. 2.6) вказана, яка кількість жил з діаметром 0,5 мм повинна бути у кабеля для підлюченя адресуючого модуля INT ADR до плати ППК INTEGRA 256 Plus.

Табл. 2.6 Кількість потрібних жил в залежності від відстані

	CK1 / CK2	DT1 / DT2	COM
Відстань	Кількість жил		
до 300 м	1	1	1
300 - 600 м	2	2	2
600- 1000 м	2	2	4

Після аналізу співвідношення кількості жил і мінімальної відстані між адресуючим модулем та платою ППК, ми визначили оптимальний кабель для наших потреб. З урахуванням відстані меншої за 300 метрів, достатньо використати

кабель з 3 жилами діаметром 0,5 мм.

Проте, зважаючи на те, що сигнал з цих модулів буде прийматись на відстані близько 1 кілометра, ми рекомендуємо використовувати кабель максимальної допустимої величини, такий як "Алай" КМлВЕеВн 8х1, який позначений червоним кольором. У цьому кабелі міститься 8 жил, і ми можемо використовувати 6 з них, залишаючи 2 жилки як резерв. Живлення для INT ADR буде забезпечуватись бесперебійним блоком живлення "Рікас-Варта".

РОЗДІЛ 3 ПРИНЦИП РОБОТИ ОХОРОННОЇ СИСТЕМИ ДУНАЙ

3.1. Вибір технічних засобів автоматизації

У нашій системі центральним елементом є контролер, він виконує керування всією системою, а також обробляє сигнали та приймає їх з датчиків, плюс до того ж може виконувати додатковий ряд завдань. AVR-ом називаються мікроконтролери, які бувають 8-ми розрядними, а також 32-розрядними, які створює компанія Atmel. Такі контролери створені на архітектурі RISC, тобто процесор має команди, які спрощені, тобто проводити додаткове шифрування не потрібно, а це у свою чергу збільшує продуктивність, знижуючи навантаження на озушку, також підсумкова вартість буде меншою через те, що використовується менше логічні елементи. Для прошивки не потрібно складного додаткового обладнання. ATmega має велику периферію, це одна з причин вибору цього сімейства. Одна з периферій це Arduino, яка являє собою пристрій для проектування інших пристроїв. Вона здатна працювати як з різними іграшками, так і з більш стоящими фізичними моделями, які можуть працювати у зв'язці з ПК, а також дозволяють застосовувати аналогові або цифрові датчики. На радість для неї є її особисте ПЗ, за допомогою якого можна легко працювати на різних системах, наприклад, Windows, Macintosh OSX, Linux, і найсмачніше те, що це ПЗ безкоштовно. Ця платформа сподобалася багатьом «радистам» через просту реалізацію, саме тому вона широко розліталася в маси. На радість для неї є її особисте ПЗ, за допомогою якого можна легко працювати на різних системах, наприклад, Windows, Macintosh OSX, Linux, і найсмачніше те, що це ПЗ безкоштовно. Ця платформа сподобалася багатьом «радистам» через просту реалізацію, саме тому вона широко розліталася в маси. На радість для неї є її особисте ПЗ, за допомогою якого можна легко працювати на різних системах, наприклад, Windows, Macintosh OSX, Linux, і найсмачніше те, що це ПЗ безкоштовно. Ця платформа сподобалася багатьом «радистам» через просту реалізацію, саме тому вона широко розліталася в маси. На радість для неї є її особисте ПЗ, за допомогою якого можна легко працювати на різних системах, наприклад, Windows, Macintosh OSX, Linux, і найсмачніше те, що це ПЗ безкоштовно. Ця платформа сподобалася багатьом «радистам» через просту реалізацію, саме тому вона широко розліталася в маси.

Arduino підходить для відтворення різних досвідчених зразків просто ідеально, хіба що потрібно вибрати з ряду, який відрізняється кількістю портів, контролером, живленням.

Найбільш популярними контролерами із сімейства ATmega можна назвати ATmega8, ATmega16, ATmega168, ATmega328P, ATmega1280, ATmega2560.

Порівняння параметрів контролерів, перерахованих вище наведено у таблиці 3.1. Хіба що для їх розуміння потрібно внести пояснення:

а) flash ROM – програмна пам'ять енергозалежна (Кбайт);

б) eeprom – комп'ютерна пам'ять енергонезалежна (Кбайт);

в) RAM - комп'ютерна пам'ять статична (байт);

г) I/O - число вступних та вивідних ліній;

д) frequency - частотна характеристика (МГц);

е) Vcc - напруги необхідне для роботи (В);

ж) Timer 8 bit – число лічильників чи таймерів 8 біт;

і) Timer 16 bit – число лічильників чи таймерів 16 біт;

к) PWM – загальна кількість каналів імпульсної модуляції, що знаходяться;

л) RTC – наявність системи реального часу;

м) SPI – модель послідовного інтерфейсу;

н) UART - кількість приймачів послідовних асинхронних;

д) AD – кількість каналів АЦП;

р) ext interrupts (Ext. Int.) - Число джерел переривання;

с) package (упаковка) – корпус та кількість висновків.

Таблиця 3.1 - Порівняльна таблиця мікроконтролерів ATmega

Параметри	Мікроконтролери ATmega					
	2560	1280	328P	168	16	8
flashROM, Кбайт	256	128	32	16	16	8
eeprom, Кбайт	4	4	1	0.5	0.5	0.5
RAM, байт	8192	8192	2048	1024	1024	1024
I/O	86	86	23	23	32	23
frequency, МГц	16	16	20	20	16	16
Vcc, В	1.8–5.5	1.8–5.5	2.7–5.5	1.8–5.5	2.7–5.5	2.7–5.5
Timer(s) 16 bit	4	4	1	1	1	1

Продовження таблиці 3.1

Timer(s) 8 bit	2	2	2	2	2	2
PWM	12	12	6	3	4	3
RTC	+	+	+	+	+	+
SPI	1	1	1+USART	1+USART	1	1
UART	4	4	1	1	1	1
AD	16	16	8	8	8	8
Ext. Int.	32	32	24	26	3	2
Package	TQFP100	TQFP100	TQFP32 PDIP28	MLF 32 PDIP 28 TQFP 32	MLF 44 PDIP 40 TQFP 44	MLF 32 PDIP 28 TQFP 32

Порівнявши дані таблиці 3.1, можна виділити ATmega 2560 і ATmega 1280, які відрізняються лише обсягом пам'яті, а також можна назвати їх флагманами цієї лінійки. Arduino Mega, повністю побудована на їх основі, має, можна сказати, найкращі технічні характеристики, а також розміри.

Датчики сигналізації: види і особливості

Завдання датчиків охоронної сигналізації — виявити присутність сторонньої людини. Сповіщувачі охоронної системи реагують на різні тригери: одні пристрої спрацьовують під час появи рухомого об'єкту, інші — під час спроби проникнути в приміщення через двері або вікно.

Систему охоронної сигналізації можна побудувати за допомогою:

- Датчиків руху;
- Датчиків вібрації;
- Герконів (датчиків відчинення дверей/вікон);
- Датчиків розбиття скла;
- Комбінованих датчиків

Рисунок 3.1 - Датчик руху Crow Swan 1000

SWAN 1000 – це комбінований пасивний інфрачервоний та мікрохвильовий детектор. Використання мікроконтролера для аналізу сигналів від піро- та мікрохвильового сенсорів дає максимальний захист від помилкових тривог. Спектральний аналіз проводиться на апаратному рівні, що робить дуже надійною детекцію.

Рисунок 3.2 - Датчик Optex Vibro

VIBRO - це інтелектуальний мікропроцесорний вібраційний детектор, або датчик вібрації. Чутливість, якого автоматично встановлюється в режимі "навчання", відповідає силі поштовхів, нанесених по поверхні, що охороняється. Таким же чином встановлюється кількість поштовхів, необхідних для появи сигналу тривоги.

Рисунок 3.3 - Геркон FM-106 (білий)

Магнітоконтактний датчик відкриття (геркон). Накладний тип установки. Робочий режим до 30 мм. Пластиковий корпус білого кольору. Дротове підключення.

Рисунок 3.4 - Датчик INDIGO

Датчик розбиття скла Satel INDIGO – призначений для використання в системі сигналізації для виявлення розбиття скла (вітрин, вікон, стелажів) на акустичному рівні. Фіксує розбиття скла: звичайного, загартованого, багатошарового, має розширений мікропроцесорний двоканальний аналіз сигналу, плавне регулювання чутливості.

Рисунок 3.5 - Кнопка тривоги Exit-EB86

Кнопка тривоги Exit-EB86 використовується з технічними засобами охоронно-пожежної або охоронної сигналізації. При натисканні вмикає сигнал тривоги.

Рисунок 3.6 - ППКОП Дунай-8/32 + Дунай-G1S

Комплект з приладу приймально-контрольного охоронно-пожежного (ППКОП) «Дунай-8/32» і модуля «Дунай-G1S», використовується для комунікації охоронно-пожежної сигналізації з ПЦС «Дунай» через мережу мобільного зв`язку. Для отримання повідомлень про пожежонебезпечну або тривожної ситуації на ППК "Дунай" задіяні 8 входів (Z1-Z8) для шлейфів охоронно-пожежної сигналізації, а з додатковими модулями розширення можливо задіяти до 128 шлейфів.

Рисунок 3.7 - Клавіатура Дунай-КА

Клавіатура «Дунай-КА» призначена для управління зовнішніми пристроями і забезпечує можливість входу на об'єкт, що охороняється і вихід з об'єкта довірених осіб без видачі сповіщень про проникнення. Клавіатура застосовується як у складі пристрою охоронної сигналізації для взяття/зняття об'єктів під охорону, так і для автономного управління виконавчими пристроями і системами контролю доступу.

З метою підвищення швидкості введення інформації та зниження економічних витрат, число N каналів джерела аналогової інформації розподіляється на n модулів введення по m аналогових каналів в кожному модулі: N=nm. Аналогові значення даних, які надходять по кожному з m каналів послідовно через аналоговий мультиплексор вводиться в мікроконтроллер. Усі n модулів введення паралельно виконують операції по введенню даних.

Відповідно до структурної схеми модуля введення на m каналів через аналоговий мультиплексор АМП кожний канал підключається на вхід аналого-цифрового перетворювача АЦП, з цифрового входа якого байт даних тимчасово записується в буферну пам’ять (БП). За сигналом зчитування ЗЧТ, який поступає з дешифратора DC байт даних з буферної пам’яті через відповідний канал цифрового мультиплексора ЦМП вводиться в мікроконтроллер. Для переключення каналів мультиплексора ЦМП і дешифратора DC із МК надходить k-розрядний код, де $k=\lg_2 n$.

Після закінчення операції перетворення аналогової величини в цифрову на виході АЦП з'являється сигнал готовності ГТ, який подається на вхід запису 3n БП і байт даних з АЦП записується в БП. Крім того, сигнал ГТ через схему затримки 1 (сигнал ГТ затримується на інтервал $t_{зап}$ часу запису даних в БП) подається на лічильний вхід двійкового лічильника СТ2 та на вхід скидання АЦП. Двійковий v-розрядний код на виході лічильника СТ2 призначений для послідовного переключання каналів аналогового мільтиплексора АМП. Число v розрядів коду переключення каналів АМП визначається формулою $v=lg_2m$

3.2.Підключення охоронної ситеми Дунай

При роботі з ППК слід дотримуватись наступних правил техніки безпеки:

- до роботи з ППК допускаються особи, які вивчили справжнє керівництво та мають посвідчення на право робіт з електроустановками до 1000 В;
- дотримуйтесь вимог ДБН В.2.5.-13-98 «ДСНУ. Інженерне обладнання будівель та споруд. Пожежна автоматика будівель та споруд»;
- не підключайте захисне заземлення до батареї опалення;
- при установці переносних вимірювальних приладів та вимірюваннях виключайте торкання струмопровідних частин з небезпечною напругою;
- при перевірці електричних ланцюгів попередньо знеструмте ці ланцюги і перевірте відсутність напруги за допомогою комбінованого приладу 43101 або йому аналогічного;
- забороняється приєднувати та відключати модулі, з'єднувачі, що знаходяться під напругою;
- забороняється включати блок живлення ППК при несправному заземленні;
- забороняється встановлювати плавкі вставки, номінали яких не відповідають документації;

- перевірити надійність підключення дроту захисного заземлення.

Заходи безпеки під час експлуатації

При роботі з приладом слід дотримуватись правил техніки безпеки, наведених у п. 2.1, а також у цьому підрозділі:

- прилади, що відмовили під час експлуатації, необхідно відновлювати шляхом заміни несправного модуля на робітник зі складу ремонтного ЗІП. Необхідність придбання ремонтного ЗІПу користувач встановлює індивідуально;
- усі роботи, пов'язані з техобслуговуванням, ремонтом та вимірюванням параметрів повинні проводитися навченим фахівцем;
- при централізованому застосуванні ППК електромонтеру ОПС необхідно попередньо повідомляти черговий пульт управління (ДПУ) про початок та завершення робіт з приладом.
- Увага, не підключайте контролбно-вимірювальну апаратуру.
- не допускайте розщеплення багатожильного дроту, що підключається, на окремі жилки, щоб уникнути замикання їх на сусідні контакти затискачів;
- при необхідності відключення мережного кабелю від приладу перевірте вольтметром відсутність на мережевому блоці затискачів напруги;
- після ретельного огляду всіх з'єднань акуратно розкладіть дроти всередині корпусів так, щоб оголені кінці дротів і екранів не торкалися радіоелементів на платі (ах), контактів акумулятора і не знаходилися в зоні підключення кабелю мережі до мережевого блоку затискачів ближче, ніж на 15 мм. Рекомендується виступають з кабелю кінці обплетення захистити ізоляцією.

Експлуатаційні обмеження

При введенні в експлуатацію та експлуатації приладу виконуйте вимоги:

- неприпустимим є підключення телефонних апаратів до лінії зв'язку на ділянці від АТС до ППК;

- не застосовуйте факси, модеми та апаратуру високочастотного ущільнення на абонентській лінії зв'язку, до якої підключено ППК;
- перед виміром опору ізоляції ланцюгів зовнішніх зв'язків необхідно їх відключити від ППК; ППК;

Встановлення ППК:

а) корпус встановити вертикально на стіні у зручному для експлуатації місці;

б) визначити місця введення кабелів у корпуси блоків;

в) витягти з корпусів необхідні введення заглушки і видалити у яких по геометрії застосовуваних коробів надлишки пластика. Встановити заглушки у корпус;

г) закріпити корпус стіні. Короби для кабелів повинні входити усередину корпусу на 3-5 мм без натягу з мінімальним зазором;

е) підключити до функціонального блоку ППК зовнішні зв'язки.

Рекомендації щодо підключення електроживлення

- Підключити мережний провід типу ПВС 2х 0,75 до мережевого блоку затискачів ППК через прохідну втулку.
- Щоб уникнути замикання дроту електроживлення на сусідні затискачі, жили оголеного на 7 - 8 мм дроти скрутити.Кінці жив не лудити!
- Після підключення проводів, мережний провід (кабель) повинен бути закріплений прохідною втулкою, що захищає кабель від переміщень та випадкового висмикування.
- Встановіть у корпус ППК акумулятор 12 В 2,4 А·ч і підключіть до нього клеми від модуля живлення (червоний провід – «+», чорний (синій) – «-»).

Таблиця 3.2 – Типи запобіжників

Призначення	Струм, А	Тип	Місце встановлення
1 У ланцюзі підключення електромережі	0,5	FSF00,5	Блок мережевих затискачів
2 У ланцюзі підключення акумулятора	1	FSF01	Під кришкою модуля живлення «Дунай-ІС05»

Рекомендації щодо централізованого застосування ППК.

При підключенні телефонної лінії до ППК виконання «Дунай-4.2» необхідно дотримуватись «полярність» лінії лише у разі застосування ППК за ручною тактикою.

Для забезпечення стійкішого прийому може бути змінено положення антени в межах її повороту. При недостатньому рівні сигналу, наведеного в антені, може бути застосована зовнішня антена з великим коефіцієнтом підсилення, призначена для застосування в частотній мережі мережі GSM900/1800. У разі не досягнення впевненого прийому, до модуля «Дунай-G1» користувачем може бути підключена виносна антена з вищим коефіцієнтом спрямованості та посилення.

Рекомендації щодо використання керуючого виходу та реле.

Вихідний комутований струм в ланцюзі виходу UK при перевантаженні обмежується позистором і становить від 0,35 до 0,5А. При призначенніреакції згідно таблиці 12 «Реле для пожежного шлейфу» та/або «UK» для пожежного шлейфу» та підключенні електроживлення активних пожежних сповіщувачів через контакти «UK» та/або контакти реле, живлення цих сповіщувачів вимикається на 4 с при тривозі по шлейфу, для якого призначено цю реакцію. За час вимкнення здійснюється скидання у вихідний стан пожежних сповіщувачів, а при включенні живлення через 2 с виконується повторний контроль стану пожежного шлейфу.

Рекомендації щодо монтажу шлейфів

Щоб запобігти деблокуванню сповіщувачів ланцюга шлейфу, вмикайте їх лише у сигнальний провід, що підключається до блоків затискачів Zi. Підключіть потай у кінці шлейфів виносний резистор опором 2,7 кОм. Резистори знаходяться у комплекті монтажних частин. В умовах сильних електромагнітних перешкод і досить довгих шлейфах (до 100 м) застосовуйте кручений екранований провід типу КОПЕВ2х2х0,4 або КОПЕВ4х2х0,4

3.3. Налаштування охоронної ситеми Дунай

ППК виконання «Дунай-1» із системним модулем «Дунай-С1041» забезпечує:

- централізоване застосування з автоматизованої тактики охорони у складі СПДІ «Дунай-XXI», «Дунай-ПРО» з передачею повідомлень на ПЦН по мережі стільникового радіозв'язку стандарту GSM900/1800 в режимі GPRS та в режимі передачі SMS;
- автономне застосування з передачею повідомлень на мобільний телефон у форматі SMS
- повідомлень мережі GSM 900/1800;
- автономне застосування.
- ППК підтримує формування одночасно до восьми каналів (напрямків) передачі даних у режимі GPRS та у форматі SMS повідомлень.
- Примітки**.**
- Одночасна передача даних між ППК та ПЦН за допомогою GPRS та за допомогою SMS –не допускається.

При централізованому застосуванні ППК у режимі передачі SMS можлива одночасна передача повідомлень на ПЦН та мобільний телефон.

Вид системного модуля «Дунай-С1041» та модуля для підключення зовнішніх зв'язків «Дунай- М1041».

Виконати конфігураціюSIM картки:

- встановити SIM-картку у мобільний телефон;
- зняти запит pin-коду згідно з посібником з експлуатації на мобільний телефон;
- видалити всі номери, у тому числі сервісні, з адресної книги SIM-картки, а також видалити всі SMS повідомлення з пам'яті SIM-картки;
- Якщо SIM карта нова, раніше ніде не використовувалася, залиште її включеною в телефоні приблизно 5 хвилин, поки

оператор стільникового зв'язку скине ВСІ SMS з налаштуваннями для GPRS, WAP і так далі, щоб їх можна було видалити.

- для передачі сповіщень на ПЦН за допомогою GPRS активувати GPRS режим у оператора мережі та вимкнути телефонію.

Якщо телефонію не вимкнути, і з яких-небудь причин на номер SIM картки йтиме телефонний дзвінок, то дані, у тому числі і тривоги, по каналу GPRS під час дзвінка не будуть передаватися.У адресну книгу SIM-картки (увага! не телефону) введіть контакти відповідно до вибраного режиму надсилання повідомлень, керуючись табл. 3.3. Контакти можна вводити лише в перші вісім осередків пам'яті адресної книги. Ім'я контакту в адресну книгу SIM картки слід вводити прописними літерами. Для передачі даних через SMS перевірити (ввести) номер SMS-центру.

Таблиця 3.3 – Режими передачі

Режим передачі	Ім'я контакту адресної книги SIM картки (ім'я напряму)	Формат запису номера до адресної книги SIM картки
1	2	3
1 Передача даних між ППК та ПЦН за допомогою GPRS з автоматичним вибором APN1)	GPRSPCO	+[дванадцять цифр IP-адреси ПЦН] 2)
2 Передача даних між ППК та ПЦН за допомогою GPRS з примусовим вибором APN1)	GPRSPCOD[код параметра]	+[дванадцять цифр IP-адреси ПЦН] 2)
3 Передача даних між ППК та ПЦН за допомогою GPRS з вибором APN1) з EEPROM (флеш-пам'яті) ППК	GPRSPCOFL	+[дванадцять цифр IP-адреси ПЦН] 2)

Продовження таблиці 3.3

4 Передача керуючих команд на ППК з телефону адміністратора ПЦН через SMS	SMSADM	+380[дві цифри коду оператора мережі] [сім цифр номера телефону адміністратора ПЦН] 3)
5 Надсилання повідомлень між ППК та ПЦН за допомогою SMS	SMSPCO	+380[дві цифри коду оператора мережі] [сім цифр номера телефону модему ПЦН] 3)
6 Передача даних між ППК та телефоном користувача за допомогою SMS	SMSUSR	+380[дві цифри коду оператора мережі] [сім цифр номера телефону користувача] 3)

У ряді випадків, таких як, наприклад, використання раніше випущених SIM карток, може знадобитися примусовий вибір точки доступу APN. У цьому випадку в адресну книгу SIM картки слід ввести ім'я GPRSPCOD[код параметра], де [код параметра] слід вибрати з (Табл. 3.3) відповідно до оператора SIM картки.

Таблиця 3.4 – Код параметра

Код параметра	Ім'я точки доступу (APN)	Оператор SIM картки
00	www.kyivstar.net	Для контрактних абонентів Kyivstar
01	www.ab.kyivstar.net	A&B Kyivstar
02	www.ab.kyivstar.net	A&B Kyivstar
03	www.djuice.com.ua	Djuice
04	www.umc.ua	МТС
05	Internet	МТС
06	Internet	МТС
07	www.jeans.ua	Jeans

Продовження таблиці 3.4

08	Internet	Life
09	internet.beeline.ua	Beeline
10	internet.beeline.ua	Beeline
11	3g.utel.ua	Utel/Beeline
---	---	---
19	M2M	Life
20	vpnl.kyivstar.net	VPN Kyivstar
21	stsb.kyivstar.net	VPN A&B Kyivstar
22	corporate.beeline.ua	Для корпоративних абонентів Beeline

З номера телефону, записаного під ім'ям SMSADM в адресній книзі SIM-картки, встановленої в ППК, адміністратор може надсилати у вигляді SMS повідомлень команди віддаленого керування на ППК. Відповіді на команди адміністратора надходять у вигляді SMS-повідомлень.

Таблиця 3.5 – Команди повідомлень

Команда(SMS повідомлення)	Варіанти написання команди(SMS повідомлення)	Результат виконання команди
1	2	3
Restart	RESTART Restart	Рестарт та взяття під охорону
Factory	FACTORY Factory	Скиданняна заводські установки
Level	LEVEL Level	Запит рівня сигналу. Отримання 16 відліків рівня сигналу протягом останніх 16 хвилин
Config	CONFIG Config	Запит версії прошивки ППК та конфігурації напрямків у SIM карті

Продовження таблиці 3.5

Gprs	GPRS Gprs	Запит стану GPRS сервісу. Відповідь: номер версії прошивки ППК та залежно від стану GPRS - **PresGprs**– GPRS є у конфігурації ППК - **AttGprs**– ППК підключено до GPRS сервісу - **ActGprs**-GPRS активовано - **ReadyGprs**– GPRS у робочому режимі - **ErrGprs**– GPRS у неробочому режимі
apn=”[точка доступу]”,”[логін]”,”[пароль]”	APN=”[точка доступу]”,”[логін]”,”[пароль]” Apn=”[точка доступу]”,”[логін]”,”[пароль]”	Запис (зміна) APN в EEPROM (флеш-пам'ять) ППК для спрямування GPRSPCOFL. Приклад команди: Apn=”stsb.kyivstar.net”,””,”" (логін та пароль оператором мобільного зв'язку не встановлено)
apn?	APN? Apn?	Запит APN з EEPROM (флеш-пам'яті) ППК
spareip=[N-1],XXX.XXX.XXX.XXX	SPAREIP=[N-1],XXX.XXX.XXX.XXX Spareip=[N-1],XXX.XXX.XXX.XXX	Встановлення резервної IP-адреси для направлення N (N – номер осередку адресної книги SIM картки від 1 до 8). Приклад команди: SPAREIP=0,202.020.020.002 (Встановити резервну IP-адресу IP202.20.20.2 для спрямування 1)

Продовження таблиці 3.5

spareip?	SPAREIP? Spareip?	Запит резервної IP-адреси. Формат відповіді: SPAREIP=[N-1],XXX.XXX.XXX.XXX (N – номер осередку адресної книги SIM картки від 1 до 8) Приклад відповіді: SPAREIP=0,213.227.202.163 (Напрямок 1, резервна IP-адреса IP213.227.202.163)
cnl=[N],"+[IP-адреса або телефон]",145,"[ім'я напряму]"	CNL=[N],"+[IP-адреса або телефон]",145,"[ім'я напряму]" Cnl=[N],"+[IP-адреса або телефон]",145,"[ім'я напряму]"	Встановлення напряму охорони номер N (N – номер осередку адресної книги SIM картки від 1 до 8). Приклад команди:CNL=1,"+202020020002",145,"GPRSPCO" (встановити IP-адресу IP202.20.20.2 для роботи ППК у режимі GPRSPCO за напрямом 1)
nssi=[номер ППК]	NSSI=[номер ППК] Nssi=[номер ППК]	Встановлення номера ППК для бази даних ПЦН (вибирається в діапазоні від 1 до 1000, заводська установка – 1)
Nssi	NSSI	Запит номера ППК для бази даних ПЦН

3.4. Перевірка роботи охоронної системи Дунай

Перевірка взяття/зняття групи під охорону. Перевірка виконується у послідовності:

- закрити дверцята корпусу ППК на ключ;
- виконати взяття/зняття групи під охорону згідно з (Табл. 3.6).

Таблиця 3.6 - Перевірка роботи охоронної системи

Операція	Послідовність виконання операцій
1	2
1 Взяття групи шлейфів під охорону	1 Клавіатуру, з якою дозволено доступ до групи, встановити режим перегляду стану групи -номер групи (приміщення). 2 Переконайтеся, що група знята з охорони (індикатор «ЗНЯТО» увімкнено) 3 Набрати на клавіатурі -код користувача. 4 Якщо у групі відсутні шлейфи із затримкою - контролювати включення індикатора «ВЗЯТО», за наявності шлейфів із затримкою індикатор увімкнеться після закінчення часу затримки (див. таблицю 22). 5 Для ППК в автономному застосуванні контролювати включення індикатора «ПІДТВ ВЗЯТТЯ».
2 Зняття групи з охорони	1 Клавіатуру, з якою дозволено доступ до групи, встановити режим перегляду стану групи, номер групи (приміщення)

Перевірка стану «Блокування взяття» виконується шляхом створення умов, наведених у п. 3 (Табл. 3.6) та для типів шлейфів, включених до групи. Контроль стану здійснюється за індикатором «ВЗЯТО» згідно з (Табл. 3.6)

Перевірка формування сповіщень виконується шляхом створення умов НОРМИ по шлейфу для якого не призначена затримка. Контроль стану здійснюється за індикаторами на клавіатурі згідно з (Табл. 3.7).

Перевірку індикації розряду акумулятора, вимкнення при повному розряді акумулятора виконати, керуючись (Табл. 3.7), формуючи відповідні умови.

Таблиця 3.7 – Перевірка індикації заряду акумулятора

Стан	Умови виникнення
1 «Час входу»	При знятті групи з охорони, коли першим порушується шлейф із затримкою типу «точка входу/шлях виходу», індикатор «ЗНЯТО» блимає з періодом 500 мс, шпаруватість 2 протягом встановленого часу затримки.
2 «Час виходу»	Після введення коду користувача індикатор «ВЗЯТО» блимає з періодом 500 мс, шпаруватість 2 протягом встановленого часу затримки. Причини формування стану: 1) до закінчення часу затримки прилад виявляє порушення шлейфу, якого затримка не призначена; 2) після закінчення часу затримки шлейф із затримкою не відновився в норму; 3) під час взяття будь-який із шлейфів опинився у стані короткого замикання.
3 «Блокування взяття»	Індикатори «ВЗЯТО» та «ПІДТВ ВЗЯТТЯ» включаються та блимають з періодом 0,5 с, шпаруватість 2 до зняття з охорони.

До початку перевірки необхідно додатково переконатися у наступному:

1) якщо ППК вводиться в експлуатацію вперше, то у чергового оператора ПЦН уточніть:

- чи заведено ППК до бази даних ПЦН;
- чи відповідає конфігурація ППК заведеної основою ПЦН;

- чи узгоджується тип «Протоколу зв'язку ППК», встановлений у базі «Дунай-4»: – «ВБД4»;
- чи виконано кросування на АТС телефонної лінії для зв'язку ППК з ПЦН.

Перевірку ППК рекомендується виконати у два прийоми:

- перевірити справність лінійної частини охоронної сигналізації, шлейфів та виконавчих пристроїв, підключених до ППК, якщо вони передбачені проектом;
- перевірити прийом/передачу формованих ППК сповіщень на ПЦН.
- Для перевірки лінійної частини необхідно в конфігурації ППК тимчасово, на час перевірки, увійти в режим програмування, вибрати функцію 1 і встановити код параметра 1 (автономне застосування ППК).
- Вийти з режиму програмування та перевірити працездатність лінійної частини, підключеної до ППК.

Для перевірки прийому/передачі формованих ППК сповіщень на ПЦН необхідно відновити у конфігурації ППК функцією 1 «вид застосування ППК», встановивши код параметра 2.

Для перевірки параметрів зв'язку ППК з ретранслятором рекомендується застосовувати наведену нижче методику:

- підключити закритий вхід осцилографа, наприклад, С1-101, до контактів «L1», «L2».
- переконатися, що ефективне значення амплітуди вхідного імпульсу від ретранслятора на контактах L1, L2 не менше 35 мВ ефф. За наявності імпульсу запиту виконати п. 2.4.3.1.6.
- за відсутності імпульсу запиту або його низькому рівні необхідно перевірити, чи правильно підключена вхідна та вихідна телефонна лінії до ППК та на ретрансляторі. Якщо підключення виконано правильно, припиніть роботи з ППК та зверніться до адміністратора ПЦН із заявкою на перевірку

кросування цієї телефонної лінії на АТС або на перевірку функціонування ретранслятора у цьому напрямку.

За наявності зв'язку індикатор «TR» коротко блимає під час обміну даними. Якщо індикатор не блимає "TR", необхідно перевірити положення двигунів потенціометрів "T", "R" на платі функціонального блоку.

Якщо й у разі немає зв'язку приладу з ПЦН - прилад несправний. За наявності зв'язку з ПЦН повторити перевірку ППК як для автономного застосування за п. 2.4.2. Імітуйте стани шлейфів та контролюйте отримання на ПЦН відповідних тривожних, заявкових та службових сповіщень по кожній групі шлейфів.

Перевірити виконання команд із ПК ПЦН:

- Опитування - отримавши цю команду, ППК повинен сформуватиповідомлення про стан шлейфів, груп та ППК на поточний момент часу та передати їх на ПЦН;
- Підтвердження для групи шлейфів – отримавши цю команду, ППК повинен для заданого номера групи увімкнути індикатор «ПІДТВ ВЗЯТТЯ»;
- Скидання ППК – ППК, отримавши цю команду, повинен виконати рестарт, сформувати повідомлення про стан шлейфів, груп і ППК на даний час і передати їх на ПЦН;
- Перевірте, що ППК запрограмований для роботи з ручною тактикою охорони, при цьому конфігурація шлейфів повинна бути встановлена за одним із кодів параметрів 5-8.

Перевірте правильність підключення зовнішніх з'єднань до ППК для організації охорони об'єкта одним або двома кордонами.

Залежно від стану шлейфів «1» – «4», взято або знято групу, відкрито або закрито дверцята, прилад може знаходитися в одному з режимів роботи:

- ППК знято з охорони;
- взяття об'єкта під охорону;
- помилки взяття під охорону;
- ППК взято під охорону;
- робота ППК у режимі «тривога»;

- переведення ППК у стан «знято»;
- контроль живлення ППК.

Нижче наведено приклад перевірки ППК для ручної тактики з використанням шлейфів у групі за кодом параметра □6□ функції 1.

Перевірка ППК у черговому режимі (група (приміщення) знята з охорони).

У цьому режимі:

- реле знеструмлено;
- в лінію зв'язку, підключену до контактів L1, L2, передається безперервний сигнал частотою
- 18 кГц;
- включений індикатор "TR", розташований на модулі "Дунай-4СМ2";
- ППК контролює цілодобовий шлейф "Z4" другого рубежу охорони;
- ППК контролює стан кнопки «ТАМПЕР», фіксуючи стан дверцят корпусу ППК
- (відкрито/закрито);
- при порушенні шлейфу "Z4":
- сигнал передачі частотою 18 кГц та індикатор «TR» вимикаються на 15 с.
- після закінчення 15 з сигнал передачі та індикатор «TR» включаються, якщо шлейф «Z4»
- відновлено у норму;
- реле вимкнено;

індикатор «ВЗЯТО» та біпер включаються з інтервалом 1 с на час затримки.

Після закінчення часу затримки на вихід ППК переводить групу (приміщення) у стан ВЗЯТО, при цьому:

- включаєтьсяреле;
- у лінію видається сигнал передачі частотою 18 кГц;

- на панелі включаються індикатори «ВЗЯТО» та «ПІДТВ ВЗЯТТЯ». Виносний індикатор підтвердження взяття під охорону, підключений до контактів «PV», дублює роботу індикатора
- «ПІДТВ ВЗЯТТЯ»;
- вмикається індикатор "TR" на модулі "Дунай-4СМ2".

Робота ППК з помилками користувача під час взяття під охорону.

При взятті під охорону об'єкта користувач може припуститися помилок, що призводять ППК до «блокування взяття» якщо за час відліку затримки:

з будь-яких причин відбулися відхилення від норми опору шлейфів Z1 - Z4 у бік короткого замикання або обрив шлейфів Z2, Z4:

- сигнал передачі частотою 18 кГц в лінію не видається;
- індикатори «ВЗЯТО» та «ПІДТВ ВЗЯТТЯ» включаються з інтервалом 0,5 с до виконання зняття з охорони групи (приміщення);

були відчинені дверцята ППК:

- реле не вмикається і сигнал передачі частотою 18 кГц у лінію не видається;
- індикатори «ВЗЯТО» та «ПІДТВ ВЗЯТТЯ»
- включаються з інтервалом 0,5 с до виконання зняття з охорони групи (приміщення);
- біпер включає звуковий сигнал з інтервалом 1 с до закриття дверцят.

Робота ППК у черговому режимі при взятій під охорону групі

Переконатися, що шлейфи «Z1» - «Z4» перебувають у нормі та індикатори «1» - «4», «ВЗЯТО», «ПІДТВ ВЗЯТТЯ» включені. У лінію видається безперервний сигнал частотою 18 кГц. Реле увімкнено.

Робота ППК при «тривозі»

У цьому режимі роботи, при порушенні будь-якого зі шлейфів Z1, Z2:

вимикається реле незалежно від того, чи відновився в норму порушений шлейф чи ні;

на панелі індикатор порушеного шлейфу блимає з періодом 250 мс протягом 15 хвилин незалежно від того, чи відновився в норму порушений шлейф чи ні. Після закінчення 15 хвилин і при відновленні шлейфу норму індикатор відповідного шлейфу включений.

При порушенні будь-якого зі шлейфів Z3, Z4:

- сигнал передачі частотою 18 кГц вимикається на (15±2), і тільки при відновленні порушеного шлейфу в стан НОРМА ППК включає сигнал передачі частотою 18 кГц;
- індикатор порушеного шлейфу блимає з періодом 250 мс протягом 15 хвилин незалежно від того, чи відновився порушений шлейф у стан НОРМА. Після закінчення цього часу та при відновленні шлейфу у стан НОРМА, індикатор відповідного шлейфу вимикається.

При відкриванні дверцят корпусу ППК біпер включає звуковий сигнал, вимикається на

15 з сигнал передавача частотою 18 кГц незалежно від положення дверцят в цей час.

При закритті дверцят біпер вимикає звуковий сигнал з інтервалом 1 с.

Перевірка ППК під час зняття з охорони групи (приміщення).

У цьому режимі роботи приладу необхідно виконати п. 2 таблиці 15. Під час зняття об'єкта з охорони вимикаються реле, індикатор «ВЗЯТО», «ПІДТВ ВЗЯТТЯ», сигнал частотою 18 кГц та індикатор «TR». Після закінчення 15 с за умови, що шлейф Z4 знаходиться в нормі, включається сигнал частотою 18 кГц і індикатор TR на модулі управління.

Контроль електроживлення ППК

При відключенні від ППК напруги електромережі 220В реле і сигнал передачі частотою 18 кГц не змінюють своїх станів.

У стані ЗНЯТО за відсутності напруги електромережі 220 В і розряд акумулятора до напруги 10,5 В, біпер включить подвійний звуковий сигнал на одну хвилину.

В стані ВЗЯТО за відсутності напруги електромережі 220 В і розряді акумулятора до напруги 10,5 В, біпер включить подвійний звуковий сигнал на одну хвилину, а передавач вимкне сигнал передавача частотою 18 кГц на 15 с.

ВИСНОВКИ

У ході виконання випускної кваліфікаційної роботи були проаналізовано теоретичні матеріали, на підставі яких був створено проект сучасної охоронно-пожежної сигналізації з віддаленим моніторинг. Під час проектування було враховано всі побажання замовника. Було спроектовано детальний план об'єкта та схеми розміщення обладнання з урахуванням нормативних документів та особливостей фінансової установи».

Зазначено, що система контролю та управління доступом потребує модернізації, яка була здійснена проектним рішенням: розроблено технічне завдання, на основі якого підібрано обладнання для восьми точок доступу. Попереднє обстеження об'єкта захисту, аналіз застосовуваних систем безпеки дозволили розробити технічне завдання на проектування охоронної системи. Було проведено порівняльний аналіз пропозицій, чотирьох зарубіжних виробників, відзначених як найбільш затребуваних споживачами. Підібрано обладнання для восьми точок доступу, а також джерела безперебійного живлення, які забезпечують нормальну роботу системи контролю та керування доступом при відключенні централізованого електропостачання. Розраховано показники надійності охоронної системи.

Технічні рішення, прийняті під час розробки охоронної системи філії банку, відповідають вимогам санітарно-гігієнічних, протипожежних та інших нормативів, що діють на території України, та забезпечують безпечне для життя та здоров'я працівників та клієнтів функціонування об'єкта при дотриманні запропонованих заходів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Актуальність сучасної системи пожежної сигналізації [Електронний ресурс] / Спектр Престиж+, 2016.

2. Корольов С.Г. Правила влаштування електроустановок. Вища школа, 2018. – 256 с.

3. Статистика пожеж/Vawilon, 2020.

4. Великі пожежі в торгових центрах та клубах України [Електронний ресурс] / Love Opium, 2018

5. Старшинов Б.П. Системи пожежної безпеки, 2013.-164 с.

6.Історія систем пожежної сигналізації [Електронний ресурс]/Спецавтоматика, 2011-2018.

7. СНіП 11-01-95. «Інструкція про склад, порядок розробки,

узгодження та затвердження проектно-кошторисної документації підприємств», 1995. - 20 с.

8. СП 4.13130.2013. Системи протипожежного захисту. Обмеження розповсюдження пожежі на об'єктах захисту. Вимоги до об'ємнопланувальних та конструктивних рішень, 2013. – 50 с

9. Randell, Brian. The Origins of Digital Computers: Selected Papers.. — 2018.

10. Hyman, Anthony. Charles Babbage, pioneer of the computer. — Oxford University Press, 2014.

11. Ralf Joost and Ralf Salomon. “Advantages of fpga-based multiprocessor systems in industrial applications”. In 31st Annual Conference of the IEEE Industrial Electronics Society (IECON 2005). IEEE-I ECON, November 2017.

12. Підприємництво і безпека. М., Універсум. 2018 р.

13. ППК «Дунай» [Інтернет джерело] Режим доступу до ресурсу: https://faraon2000.com/ua/p74525843-ppk-dunaj-832.html (дата звернення: 20.05.2023)

14. Датчик INDIGO [Інтернет джерело] Режим доступу до ресурсу: https://www.bezpeka-shop.com/product/datchik-indigo/ (дата звернення: 20.05.2023)

15. Датчик руху [Інтернет джерело] Режим доступу до ресурсу: https://crow.ua/ru/products/swan-1000 (дата звернення: 20.05.2023)

16. Датчик відкриття [Інтернет джерело] Режим доступу до ресурсу: https://ohrana.ua/datchiki/magnitno-kontaktniy-datchik-tane-fm-106-beliy.html (дата звернення: 20.05.2023)