

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

*Спеціальність: 123 «Комп'ютерна інженерія»*

*Освітньо-професійна програма: «Обслуговування  
комп'ютерних систем і мереж»*

*Група: 4КС-57*

# **Дипломний проект**

**здобувача освіти денної форми навчання  
КС.57.19.000.ДП**

***СВИРИДИ ОЛЕКСАНДРА  
ОЛЕКСАНДРОВИЧА***

**м. Одеса  
2024 р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КС-57

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

до дипломного проекту на тему:

**Розробка системи охоронної сигналізації офісу**

Проектний матеріал складається з пояснювальної записки на 65 сторінках та графічного (презентаційного) матеріалу на 11 аркушах (слайдах)

Дипломник \_\_\_\_\_ (Свирида О.О.)  
Керівник \_\_\_\_\_ (Кільдішев В.Й.)

**Консультанти:**

з економічного розділу \_\_\_\_\_ (Іванченков В.С.)  
з розділу охорони праці та техніки безпеки \_\_\_\_\_ (Чорновол Н.І.)  
з нормоконтролю \_\_\_\_\_ (Петрашова В.І.)  
старший консультант \_\_\_\_\_ (Кривченко Ю.В.)

**До захисту допущений**

Голова циклової комісії \_\_\_\_\_ (Кривченко Ю.В.)  
Завідувач відділення \_\_\_\_\_ (Скорнякова О.В.)

Захист «21» 06 2024 р.      Протокол ЕК № 5  
Оцінка ЕК 4/добре 75.5

Секретар ЕК \_\_\_\_\_

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

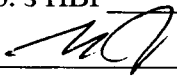
Відділення комп'ютерних систем Комісія КТ та ПІ

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма « Обслуговування комп'ютерних систем і мереж»

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

  
« 15 » 01 2024 р.

**ЗАВДАННЯ**

**на дипломний проект**

Здобувачеві освіти: Свириді Олександр Олександровичу

1. Тема проекту: Розробка системи охоронної сигналізації офісу.

Затверджена наказом по коледжу від « 2 » 11 202 3р. № 244-А2-00

2. Термін здачі закінченого проекту «10» червня 2024 р.

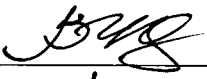
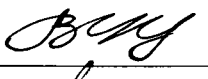


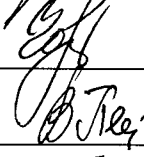
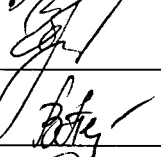
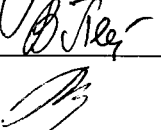
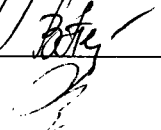


3. Вихідні дані до проекту:

1. Вимоги до системи охоронної сигналізації офісу.
2. Датчики для системи охоронної сигналізації.
3. Застосування платформи Arduino для розробки проекту.
4. Розробити схема електричну принципіальну системи охоронної сигналізації офісу.
5. Реалізація та моделювання працездатності проекту.



4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити):  
Основні компоненти системи охорони об'єктів; Складові системи охоронної сигналізації;  
Пристрої управління для системи охоронної сигналізації; Аналіз плану офісу для  
розміщення датчиків охоронної сигналізації; Схема електрична системи охоронної  
сигналізації; Розробка і реалізація системи охоронної сигналізації офісу; Економічні  
розрахунки; Заходи ТБ.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів): Компоненти системи охоронної сигналізації офісу; Пристрої  
управління системи охоронної сигналізації офісу; План офісу; Розташування пристроїв  
охоронної сигналізації офісу; Обґрунтування вибору мікроконтролера Arduino для  
системи охоронної сигналізації; Комплектуючі елементи для системи охоронної  
сигналізації офісу; Пристрої та обладнання для системи охоронної сигналізації офісу;  
Зображення кінцевого результату роботи.


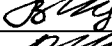
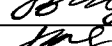
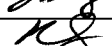











6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується



Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	Кільдішев В.Й.		
Економічний розділ	Іванченков В.С.		
Розділ охорони праці	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		
Старший консультант	Кривченко Ю.В.		

7. Дата видачі завдання: «15» 01 2024 р.

Керівник Кільдішев В.Й.  (підпис)  
 Завдання прийняв до виконання Свирида О.О.  (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Вступ. Постановка мети та задач проектування.	23.04.24	
2	Вивчення технічної документації.	13.05.24	
3	Опис принципів реалізації СКУД.	20.05.24	
4	Аналіз роботи технології iButton.	24.05.24	
5	Аналіз роботи технології Arduino.	25.05.24	
6	Дослідження алгоритмів роботи СКУД.	26.05.24	
7	Створення алгоритму роботи системи.	28.05.24	
8	Вибір компонентів для розробки системи.	30.05.24	
9	Розробка програмного забезпечення Arduino.	01.05.24	
10	Тестування функцій пристроїв.	02.05.24	
11	Виявлення та виправлення помилок.	03.06.24	
12	Аналіз результатів, підготовка презентації.	05.06.24	
13	Економічні розрахунки та питання з ОП.	06.06.24	
14	Підготовка графічної частини проекту.	07.06.24	
15	Підготовка проекту до захисту та тестування.	10.06.24	

Дипломник  (підпис)  
 Керівник  (підпис)



# ЗМІСТ

Вступ.....	7
1 Основний розділ .....	8
1.1 Теоретичні аспекти розробки системи охоронної сигналізації офісу	8
1.1.1 Історичний огляд розвитку систем охоронної сигналізації...	8
1.1.2 Огляд сучасних систем охоронної сигналізації .....	10
1.1.3 Визначення вимог до системи охоронної сигналізації офісу.	11
1.1.4 Технології та принципи побудови системи охоронної сигналізації .....	13
1.1.5 Нормативно-правове забезпечення встановлення та експлуатації системи охоронної сигналізації.....	14
1.2 Аналіз існуючих рішень .....	16
1.2.1 Сучасні ринкові пропозиції систем охоронної сигналізації ...	16
1.2.2 Оцінка переваг та недоліків існуючих систем .....	26
1.2.3 Аналіз вимог до системи охорони периметру об'єкту .....	31
1.3 Проектування системи охоронної сигналізації офісу.....	32
1.3.1 Вибір технічних засобів системи .....	32
1.3.2 Доцільність застосування платформи Arduino для проектування системи сигналізації офісу .....	33
1.3.3 Розробка системи охорони сигналізації офісу .....	34
1.3.4 Цифровий модуль датчика нахилу .....	36
1.3.5 Розробка схеми електричної принципальної системи охоронної сигналізації.....	38
1.3.6 Розробка програмного забезпечення системи охоронної сигналізації.....	42
2 Економічний розділ.....	48
2.1 Резюме.....	48
2.2 Розрахунок ціни програмного продукту нормативним методом..	48

2.2.1	Визначення трудомісткості розробки програмного забезпечення.....	48
2.2.2	Розрахунок ціни програмного продукту.....	52
3	Розділ охорони праці та техніка безпеки.....	55
3.1	Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці програмного комплексу.....	55
3.2	Гігієнічні вимоги до виробничого середовища.....	55
3.2.1	Вимоги до приміщення.....	56
3.2.2	Освітлення.....	56
3.2.3	Шум.....	56
3.2.4	Мікроклімат.....	56
3.2.5	Електробезпека.....	57
3.2.6	Вимоги до організації робочого місця працівника.....	57
3.3	Пожежна безпека.....	59
	Висновки.....	60
	Перелік використаних інформаційних джерел.....	61
	Додаток А. Слайди мультимедійної презентації.....	62

## ВСТУП

Історичний огляд розвитку систем охоронної сигналізації свідчить про поступовий еволюційний процес в цій сфері, який відбувався на протязі багатьох десятиліть. Перші системи охоронної сигналізації виникли у середньовіччі, коли для сигналізації про наближення ворожого вторгнення використовувалися дзвінки, димові сигнали та сигнальні вогні. У 17-18 століттях були створені перші прості механічні пристрої, що реагували на відкриття дверей або вікон.

У 19-20 століттях з появою електрики стали поширюватися системи охоронної сигналізації, що базувалися на використанні електричних схем, датчиків та сирен. Такі системи використовувалися переважно для захисту від крадіжок у комерційних та промислових приміщеннях.

У другій половині 20 століття з'явилися цифрові системи охоронної сигналізації, які були більш надійними та функціональними. Ці системи використовували мікроконтролери та програмне забезпечення для керування та моніторингу безпеки об'єктів. Використання мікроконтролерів дозволило створювати компактні пристрої для керування та моніторингу безпеки. Ці пристрої забезпечували високу швидкість обробки даних та можливість програмування різних режимів реагування на події. Розвиток програмного забезпечення для цифрових систем охоронної сигналізації дозволяв реалізувати різноманітні функції, включаючи моніторинг стану об'єкту в режимі реального часу, віддалене керування та налаштування системи, а також аналіз подій та генерацію звітів. З'явлення цифрових систем дало змогу використовувати різноманітні комунікаційні протоколи, такі як Ethernet, Wi-Fi, GSM, для забезпечення зв'язку між компонентами системи та зовнішнім світом.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		7

# 1 ОСНОВНИЙ РОЗДІЛ

## 1.1 Теоретичні аспекти розробки системи охоронної сигналізації офісу

### 1.1.1 Історичний огляд розвитку систем охоронної сигналізації

Цифрові системи охоронної сигналізації мали широкий спектр функціональних можливостей, включаючи виявлення руху, контроль доступу, інтеграцію з системами відеоспостереження та автоматизованими системами управління будівлями.

Використання цифрових технологій дозволило покращити надійність систем охоронної сигналізації шляхом мінімізації помилок та інтерференції, а також швидкого виявлення та реагування на події.

Отже, впровадження цифрових систем охоронної сигналізації в другій половині 20 століття відкрило нові можливості для забезпечення безпеки об'єктів та зробило їх більш ефективними та надійними.

У сучасному світі системи охоронної сигналізації стали невід'ємною частиною життя в багатьох сферах, включаючи промисловість, комерцію, а також приватний сектор. Вони постійно вдосконалюються за допомогою новітніх технологій, таких як штучний інтелект, IoT та хмарні обчислення.

У великих промислових підприємствах системи охоронної сигналізації відіграють ключову роль у запобіганні аварій, виявленні пожеж та реагуванні на них, контролі доступу до небезпечних зон, а також в моніторингу стану обладнання та інфраструктури.

У бізнесі системи охоронної сигналізації використовуються для захисту від крадіжок, вломів, витоку конфіденційної інформації, а також для контролю за працівниками та відвідувачами.

В домашніх умовах системи охоронної сигналізації забезпечують захист від втручання в особисте простір, виявлення пожеж та інших небезпечних

					КС 57. 19 000. 00 ДП ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		8

ситуацій, а також можуть включати функції автоматизації, такі як керування освітленням, опаленням, системами кондиціонування тощо. Щоб вдосконалювати ефективність та функціональність систем охоронної сигналізації, сьогодні активно використовуються новітні технології.

Штучний інтелект (AI) дозволяє системам аналізувати великі обсяги даних, розпізнавати аномальну поведінку та автоматично реагувати на потенційні загрози.

Використання інтернет речей (IoT): за допомогою IoT сенсорів та пристроїв системи можуть бути підключені до мережі Інтернет, що дозволяє віддалено керувати та моніторити безпеку об'єктів.

Використання хмарних технологій дозволяє зберігати та обробляти дані з більшою ефективністю та доступністю, а також забезпечує можливість використовувати розподілені ресурси для обробки інформації.

Загалом, сучасні системи охоронної сигналізації постійно розвиваються, стаючи все більш інтелектуальними, автоматизованими та інтегрованими, що дозволяє забезпечити більшу безпеку та контроль над об'єктами в будь-яких умовах.

Майбутній розвиток систем охоронної сигналізації передбачає ряд інноваційних та технологічних тенденцій, які спрямовані на поліпшення їх функціональності, ефективності та інтеграції з іншими системами "розумних будівель". Деякі з цих тенденцій включають:

1) інтеграція з іншими системами "розумних будівель": системи охоронної сигналізації все більше починають взаємодіяти з іншими системами управління будівлями, такими як системи автоматизації освітлення, опалення, кондиціонування повітря, а також системи контролю доступу та відеоспостереження. Це дозволяє створювати інтегровані "розумні" середовища, які забезпечують більшу ефективність та зручність управління;

2) розширення можливостей моніторингу та аналізу даних: за допомогою передових аналітичних технологій, таких як штучний інтелект та машинне навчання, системи охоронної сигналізації зможуть аналізувати великі обсяги

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		9

даних, виявляти відхилення в поведінці та прогнозувати можливі загрози. Це дозволить вчасно реагувати на потенційні небезпеки та запобігати виникненню аварійних ситуацій;

3) використання передових технологій: майбутнє систем охоронної сигналізації передбачає використання передових технологій, таких як датчики зі штучним інтелектом, блокчейн, квантові обчислення та інші інновації. Ці технології можуть забезпечити більшу точність, швидкість та безпеку в роботі систем охоронної сигналізації;

4) збільшення автоматизації та інтелектуалізації: завдяки розвитку штучного інтелекту та інтернету речей, системи охоронної сигналізації стають все більш автоматизованими та інтелектуальними. Вони можуть автоматично реагувати на події, виконувати прогнозування та аналізувати дані для прийняття оптимальних рішень;

Отже, майбутні розвиток систем охоронної сигналізації спрямований на створення ще більш інтегрованих, ефективних та інтелектуальних рішень, які забезпечать вищий рівень безпеки та комфорту для користувачів.

### **1.1.2 Огляд сучасних систем охоронної сигналізації**

Огляд сучасних систем охоронної сигналізації може включати наступні пункти:

1) типи систем охоронної сигналізації:

- проводові системи: базуються на дротяних з'єднаннях між датчиками, сенсорами та центральною системою керування;

- бездротові системи: використовують радіосигнали для зв'язку між компонентами, що робить їх встановлення більш простим та гнучким;

2) основні компоненти системи:

- датчики руху та відкриття: реагують на незаконне проникнення або рух у визначених зонах;

- камери відеоспостереження: дозволяють відстежувати події у реальному часі та записувати їх для подальшого аналізу;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		10

- сирени та світлові сигнали: використовуються для візуального та акустичного попередження про порушення безпеки;

- центральна система керування: обробляє інформацію від датчиків та приймає рішення щодо активації сигналів тривоги;

3) технологічні рішення:

- інтеграція з мобільними додатками: дозволяє користувачам отримувати сповіщення про події та керувати системою віддалено через смартфони або планшети;

- штучний інтелект та аналітика даних: застосовуються для виявлення аномальної активності та покращення точності реагування системи на потенційні загрози;

- хмарні рішення: дозволяють зберігати та обробляти дані в онлайн-режимі, забезпечуючи доступ до них з будь-якої точки з'єданого пристрою;

4) тенденції розвитку:

- зростання використання IoT (інтернету речей) для забезпечення сполучення між різними пристроями системи;

- збільшення використання аналітики даних для передбачення подій та оптимізації роботи системи;

- розширення можливостей інтеграції з іншими системами безпеки та автоматизації офісного простору.

Огляд сучасних систем охоронної сигналізації допоможе визначити технологічні та функціональні вимоги до розроблюваної системи для офісного середовища.

### **1.1.3 Визначення вимог до системи охоронної сигналізації офісу**

Визначення вимог до системи охоронної сигналізації офісу є ключовим етапом у процесі проектування та розробки такої системи (рис. 1.1). Нижче наведено список основних вимог, які можуть бути враховані при розробці системи охоронної сигналізації для офісного приміщення:

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>11</b>

1) забезпечення безпеки персоналу: система повинна надавати ефективний захист від небажаних вторгнень, крадіжок та інших небезпечних ситуацій, що можуть загрожувати персоналу офісу;

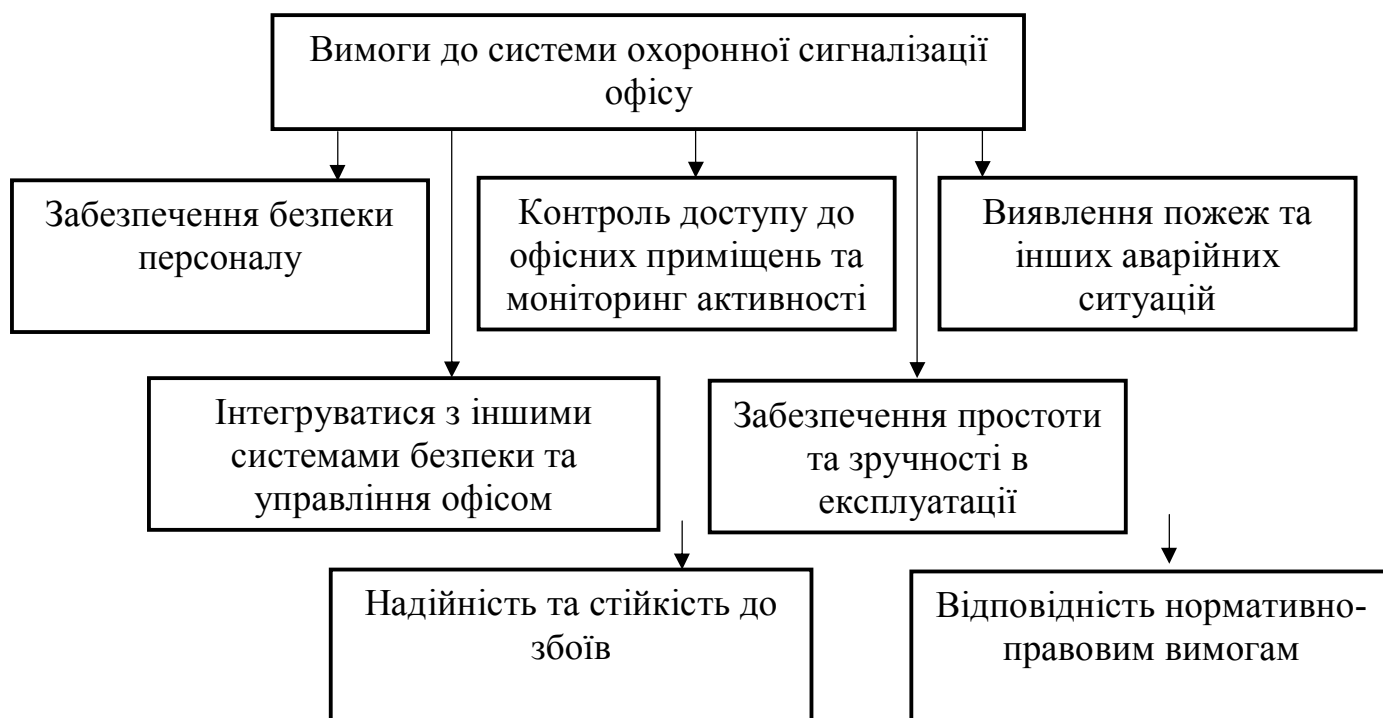


Рисунок 1.1. Основні вимог до системи охоронної сигналізації офісу

2) захист майна: система повинна забезпечувати контроль доступу до офісних приміщень та моніторинг активності, щоб запобігти крадіжкам майна та вандалізму;

3) виявлення пожеж та інших аварійних ситуацій: система повинна мати можливість виявлення пожежі, витоку газу, затоплення та інших небезпечних ситуацій і надавати відповідний сигнал тривоги для оперативного реагування персоналу та екстрених служб;

4) інтеграція з іншими системами: система повинна бути здатною інтегруватися з іншими системами безпеки та управління офісом, такими як системи відеоспостереження, системи контролю доступу, системи управління освітленням та кондиціонуванням повітря тощо;

5) забезпечення простоти та зручності в експлуатації: система повинна бути легкою у встановленні, налаштуванні та керуванні, а також мати інтуїтивний і зрозумілий інтерфейс для користувачів;

6) надійність та стійкість до збоїв: система повинна бути надійною та стійкою до збоїв, а також мати резервні джерела живлення та можливість автоматичного відновлення роботи після відновлення живлення;

7) відповідність нормативно-правовим вимогам: система повинна відповідати всім вимогам законодавства та стандартам щодо охорони праці та безпеки працівників.

Ці вимоги можуть бути деталізовані та доповнені в залежності від конкретних потреб та особливостей офісного приміщення. Важливо також забезпечити взаємодію з представниками персоналу та замовниками, щоб зрозуміти їхні вимоги та очікування від системи охоронної сигналізації.

#### **1.1.4 Технології та принципи побудови системи охоронної сигналізації**

Система охоронної сигналізації базується на різноманітних технологіях та принципах, які спільно допомагають забезпечити безпеку приміщення. Нижче подано деякі з найважливіших технологій та принципів, які використовуються у побудові систем охоронної сигналізації:

1) датчики руху та контактні датчики: ці пристрої виявляють рух або відкриття дверей і вікон. Вони активують сигнал тривоги, коли реєструють незвичайну активність в зоні моніторингу;

2) камери відеоспостереження: камери дозволяють в реальному часі моніторити події в приміщенні і зберігати записи для подальшого аналізу. Вони можуть бути використані для виявлення незвичайної або підозрілої активності.

3) сенсори диму та вуглекислого газу: ці датчики виявляють наявність диму або небезпечних газів у приміщенні і спрацьовують тривогу, щоб попередити про можливу пожежу або іншу аварійну ситуацію.

4) сирени та світлові сигнали: ці пристрої використовуються для негайного повідомлення персоналу про тривожні ситуації. Вони можуть видавати гучний звуковий сигнал та/або вмикають яскраві світлові сигнали для привернення уваги;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		13

5) контролери доступу: ці системи встановлюють правила доступу до приміщення та контролюють рух людей. Вони можуть використовувати картки доступу, PIN-коди або біометричні дані для ідентифікації осіб;

6) центральний контроль та моніторинг: централізована система керування дозволяє моніторити всі підсистеми охоронної сигналізації, приймати рішення та вживати заходів в разі спрацювання тривоги;

7) віддалене керування та моніторинг: сучасні системи охоронної сигналізації можуть бути віддалено керовані та моніторені через мобільні додатки або веб-інтерфейси;

8) інтеграція з іншими системами: системи охоронної сигналізації часто інтегруються з іншими системами безпеки та управління будівлями, такими як системи контролю доступу, системи відеоспостереження, системи управління освітленням і кондиціонуванням повітря тощо.

Ці технології та принципи допомагають створити повноцінну систему охоронної сигналізації, яка ефективно захищає приміщення та його персонал від різних небезпек.

### **1.1.5 Нормативно-правове забезпечення встановлення та експлуатації системи охоронної сигналізації**

Встановлення та експлуатація системи охоронної сигналізації підпадає під регулювання різних нормативно-правових актів, які можуть варіюватися в залежності від країни та регіону. Нижче наведені деякі загальні принципи та нормативні вимоги, які зазвичай враховуються при встановленні та експлуатації систем охоронної сигналізації:

1) будівельні норми та стандарти: встановлення системи охоронної сигналізації повинно відповідати відповідним будівельним нормам та стандартам, які регулюють питання безпеки та захисту будівель та споруд;

2) пожежна безпека: встановлення системи охоронної сигналізації повинно дотримуватися вимог щодо пожежної безпеки, включаючи встановлення датчиків диму та вуглекислого газу, а також сирен та інших пристроїв тривоги;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		14

3) електробезпека: при встановленні та експлуатації системи охоронної сигналізації необхідно дотримуватися відповідних норм та правил електробезпеки, щоб уникнути можливих аварій та загроз для персоналу;

4) державні норми та регулювання: у багатьох країнах існують державні нормативи та правила, які регулюють встановлення та експлуатацію систем охоронної сигналізації. Ці нормативи можуть включати вимоги до сертифікації обладнання, процедур аудиту та технічного обслуговування;

5) законодавство щодо захисту даних: з урахуванням того, що системи охоронної сигналізації можуть збирати та обробляти особисті дані, важливо дотримуватися відповідних законодавчих вимог щодо захисту даних та конфіденційності;

6) норми щодо праці: встановлення та експлуатація системи охоронної сигналізації повинні дотримуватися відповідних норм щодо охорони праці та безпеки працівників, включаючи навчання персоналу та виконання процедур евакуації в разі аварійних ситуацій;

7) місцеві правила та регуляції: у деяких випадках можуть існувати місцеві правила та регуляції, які стосуються встановлення та експлуатації систем охоронної сигналізації, які також потрібно враховувати.

Враховуючи ці нормативні вимоги та принципи, можна забезпечити встановлення та експлуатацію системи охоронної сигналізації відповідно до вимог безпеки та законодавства.

В Україні встановлення та експлуатація систем охоронної сигналізації регулюються рядом нормативно-правових актів. Основні з них включають:

1) будівельний кодекс України: вимоги до систем охоронної сигналізації можуть бути визначені відповідними розділами Будівельного кодексу України, який містить стандарти та вимоги щодо будівельної безпеки;

2) норми електробезпеки: з урахуванням електричної складової систем охоронної сигналізації, важливо дотримуватися норм та правил електробезпеки, зокрема СНиП 3.05.06-85 "Електрообладнання" та інших відповідних нормативно-правових актів;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>15</b>

3) нормативні документи щодо пожежної безпеки: встановлення системи охоронної сигналізації також пов'язане з вимогами до пожежної безпеки, які можуть бути визначені відповідними нормативними документами, такими як Правила пожежної безпеки в Україні;

4) законодавство щодо захисту даних: оскільки системи охоронної сигналізації можуть збирати та обробляти особисті дані, важливо дотримуватися відповідних законодавчих вимог щодо захисту даних та конфіденційності, таких як Закон України "Про захист персональних даних";

5) нормативи щодо охорони праці: встановлення та експлуатація системи охоронної сигналізації повинні дотримуватися відповідних норм щодо охорони праці та безпеки працівників, які можуть бути визначені Законом України "Про охорону праці" та іншими відповідними актами;

6) ліцензування та сертифікація: у зв'язку з діяльністю з встановлення та обслуговування систем охоронної сигналізації може бути вимагане ліцензування та сертифікація, зокрема відповідно до Закону України "Про ліцензування видів господарської діяльності".

Ці нормативно-правові акти визначають вимоги та правила, які потрібно враховувати при встановленні та експлуатації систем охоронної сигналізації в Україні. Дотримання цих вимог є важливим для забезпечення високого рівня безпеки та відповідності законодавству.

## **1.2 Аналіз існуючих рішень**

### **1.2.1 Сучасні ринкові пропозиції систем охоронної сигналізації**

На сучасному ринку існує велика кількість різних систем охоронної сигналізації, які пропонуються відомими компаніями з безпеки. Ось кілька сучасних пропозицій:

1) системи "розумного будинку" зі вбудованою охоронною сигналізацією можуть включати датчики руху, дверей та вікон, камери відеоспостереження, димові та вуглекислотні детектори, які підключаються до центрального

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>16</b>

контролера. Вони надають можливість віддаленого керування через мобільний додаток, а також сповіщення в реальному часі про події в будинку;

2) бездротові системи охоронної сигналізації: ці системи легко встановлюються, оскільки вони не потребують прокладання дротів. Вони включають в себе датчики руху, віконні та дверні контактори, а також звукові і оптичні сигналізатори. Багато з них можуть бути інтегровані з системами "розумного будинку";

3) системи відеоспостереження зі вбудованими функціями охоронної сигналізації включають камери відеоспостереження з функціями виявлення руху та обличчя, а також можливість надсилання сповіщень в разі виявлення підозрілих об'єктів або дій;

4) системи з контролем доступу використовуються для обмеження доступу до певних зон або приміщень. Такі системи можуть включати карткові чи біометричні читачі, дверні замки з вбудованим електронним керуванням, а також системи відеоспостереження для контролю доступу;

5) хмарні системи охоронної сигналізації зберігають дані та відеозаписи в хмарних серверах, що дозволяє власникам отримувати доступ до них з будь-якої точки, де є Інтернет;

6) системи інтегрованого безпекового керування об'єднують в собі охоронні системи, контроль доступу, відеоспостереження та інші функції безпеки в єдину інтегровану систему керування.

Ці пропозиції відображають сучасні тенденції в розробці систем охоронної сигналізації, які стають все більш інтелектуальними та пристосованими до потреб користувачів.

Системи "розумного будинку" з вбудованою охоронною сигналізацією є одними з найбільш сучасних і зручних варіантів для забезпечення безпеки вашого будинку. Ось деякі ключові функції цих систем:

1) датчики руху реагують на рух в будинку і можуть надсилати сповіщення власникам або включати сигналізацію;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		17

2) дверні та віконні датчики виявляють відкриття або закриття дверей та вікон, а також можуть надсилати сповіщення про незаконне відкриття;

3) камери відеоспостереження не лише записують відео, але і можуть виявляти рух, а також надсилати сповіщення в разі виявлення підозрілих об'єктів або дій;

4) димові та вуглекислотні детектори виявляють пожежу або викиди газу і включають сигналізацію, а також надсилають сповіщення;

5) віддалене керування через мобільний додаток: власники можуть контролювати систему охорони та отримувати сповіщення з будь-якого місця, де є Інтернет;

6) інтеграція з іншими "розумними" пристроями: системи можуть бути інтегровані з освітленням, термостатами, розетками і багатьма іншими пристроями, що дозволяє автоматизувати роботу будинку для підвищення безпеки та зручності;

7) сповіщення в реальному часі: власники можуть отримувати сповіщення про будь-які події в будинку в реальному часі, такі як відкриття дверей або виявлення руху;

8) запис відео: багато систем здатні записувати відео на внутрішній або зовнішній накопичувач, що дозволяє вам переглядати події, що відбуваються в будинку.

Ці системи можуть бути легко встановлені та налаштовані і забезпечують високий рівень безпеки та контролю над вашим будинком.



Рисунок 1.1. ПЧ сповіщувач руху DSC LC-100

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		18



Рисунок 1.3. Магнітоконтант TANE sm-35



Рисунок 1.4. Сповіщувач пожежний Артон СПД-3



Рисунок 1.5. Вібраційний датчик DSC STIMSHOCK-01

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
						19
Зм.	Арк.	№ докум.	Підпис	Дата		

Бездротові системи охоронної сигналізації стали дуже популярними через їхню простоту встановлення та високий рівень ефективності. Ось кілька ключових особливостей таких систем:

1) простота встановлення: бездротові системи не потребують прокладання кабелів, що значно спрощує процес встановлення. Це дозволяє швидко встановлювати систему без спеціалізованих знань або допомоги фахівців;

2) портативність: бездротові датчики можуть бути легко перенесені з одного місця в інше, що дозволяє змінювати конфігурацію системи в залежності від потреб;

3) низька вартість: бездротові системи зазвичай менш коштовні в порівнянні з проводовими системами, оскільки не потребують витрат на матеріали та працю з прокладанням кабелів;

4) гнучкість в конфігурації: можна додавати або видаляти компоненти системи з легкістю, наприклад, додавати додаткові датчики або камери, якщо це потрібно;

5) надійність: сучасні бездротові системи використовують захищені протоколи зв'язку, які роблять їх менш вразливими до перешкод або втручання;

6) мобільне керування: багато бездротових систем охоронної сигналізації мають мобільні додатки, що дозволяють керувати системою та отримувати сповіщення через смартфон або планшет;

7) інтеграція з іншими "розумними" пристроями: бездротові системи можуть легко інтегруватися з іншими "розумними" пристроями в будинку, такими як освітлення, термостати та інші, для автоматизації різних аспектів вашого життя.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		20



Рисунок 1.6. Бездротовий датчик руху AJAX MotionProtect Plus White

Загалом, бездротові системи охоронної сигналізації є зручним та надійним рішенням для багатьох власників будинків та бізнесів. Вони пропонують високий рівень безпеки та зручності за доступну ціну.



Рисунок 1.7. Брелок для управління охоронною системою AJAX SpaceControl White

					КС 57. 19 000. 00 ДП ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		21

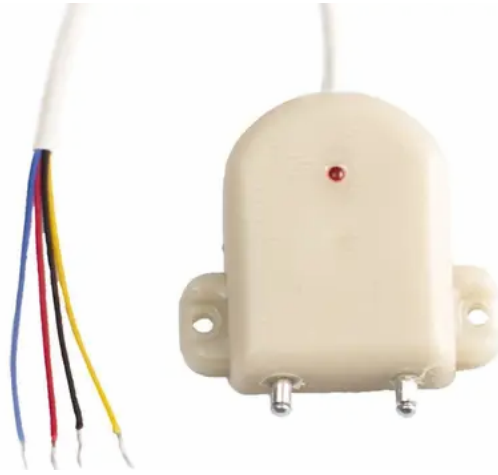


Рисунок 1.8. Датчик затоплення Geos SW-1

Системи відеоспостереження зі вбудованими функціями охоронної сигналізації надають вам не лише можливість відслідковувати події, що відбуваються, а й реагувати на них у реальному часі. Ось кілька ключових функцій таких систем:

1) виявлення руху: вбудовані датчики руху можуть виявляти навіть найменші рухи в зоні спостереження. Це дозволяє спостерігати за незвичайними подіями, такими як вторгнення чи намагання відкрити двері;

2) сповіщення в реальному часі: системи можуть надсилати сповіщення на ваш смартфон або інший пристрій, коли виявляється підозріла діяльність;

3) запис відео з подіями: система може автоматично почати запис відео, коли виявляється рух або інша підозріла активність. Це дозволяє вам переглядати події, які сталися, а також зберігати їх для подальшого аналізу або доказів;

4) виявлення обличчя: деякі системи можуть виявляти обличчя та розпізнавати відомі особи, що дозволяє вам стежити за тим, хто перебуває в вашому приміщенні;

5) інтеграція з іншими системами безпеки: відеоспостереження може бути інтегроване з іншими системами безпеки, такими як датчики руху, дверні датчики та сигналізація, для створення комплексної системи безпеки;

6) віддалене керування та перегляд: можна віддалено переглядати відео з камер та керувати системою через мобільний додаток, навіть якщо ви не вдома;

7) зберігання в хмарі: відеозаписи можуть зберігатися в хмарних сервісах, що дозволяє легко отримувати до них доступ з будь-якої точки з Інтернетом і зберігати дані в безпеці;

8) аналітика відео: деякі системи можуть аналізувати відео для виявлення певних подій, таких як рух об'єктів або відсутність руху в певних зонах.

Ці системи забезпечують високий рівень безпеки та контролю, а також можливість реагувати на події в реальному часі, що дозволяє вам залишатися впевненими в безпеці вашого приміщення.

Системи з контролем доступу використовуються для обмеження доступу до певних зон або приміщень, забезпечуючи безпеку та контроль над об'єктом. Ось деякі ключові функції цих систем:

1) карткові читачі дозволяють використовувати магнітні або безконтактні картки для відкриття дверей чи в'їзду на територію;

2) біометричні читачі використовують біометричні дані (наприклад, відбитки пальців, розпізнавання обличчя) для ідентифікації користувача;

3) дистанційне керування: адміністратори систем можуть віддалено керувати доступом, змінювати права доступу або блокувати картки/акаунти;

4) аудит доступу: системи зберігають журнали доступу, які вказують, хто, коли і де використовував свої карти або біометричні дані;

5) множинний рівень доступу: дозволяє налаштовувати рівні доступу для різних користувачів або груп користувачів;

6) автоматичне блокування: системи можуть автоматично блокувати доступ після певної кількості невдалих спроб введення коду або біометричних даних;

7) інтеграція з відеоспостереженням: можливість інтеграції з системами відеоспостереження для запису відвідувань та взаємозв'язку з подіями;

8) захист від обману: сучасні системи мають заходи безпеки, які захищають від обману, такі як клонування карток;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		23

9) мобільний доступ: деякі системи дозволяють використовувати мобільні пристрої для вхідного контролю через NFC або Bluetooth;

10) гнучкість у встановленні: вони можуть бути встановлені в різних типах об'єктів – від малих офісів до великих підприємств або навіть житлових будинків.

Ці системи забезпечують високий рівень безпеки та контролю доступу, що дозволяє ефективно керувати фізичною безпекою будь-якого об'єкту.

Хмарні системи охоронної сигналізації – це передові рішення, які використовують хмарні технології для збереження даних та керування безпекою. Ось деякі особливості та переваги цих систем:

1) віддалений доступ: можна контролювати та керувати своєю системою охорони з будь-якої точки, де є доступ до Інтернету. Це означає, що ви можете перевіряти статус системи, дивитися відеопотік з камер, отримувати сповіщення про події тощо через мобільний додаток або веб-портал;

2) безпечне збереження даних: всі відеозаписи та дані системи зберігаються у віддалених хмарних серверах, що гарантує безпеку ваших даних та захищає їх від втрати чи пошкодження;

3) сповіщення в реальному часі: хмарні системи надсилають сповіщення в реальному часі на ваш мобільний телефон або інші пристрої, якщо відбувається подія, яка потребує вашої уваги, наприклад, спрацювання датчика руху або виявлення пожежі;

4) легкість у встановленні та розширенні: більшість хмарних систем пропонують бездротові компоненти, що значно спрощує процес встановлення. Ви також можете легко розширити систему, додавши нові датчики, камери чи інші пристрої;

5) автоматизація та інтеграція: можна налаштувати автоматичні правила та сценарії, які реагують на певні події, наприклад, автоматично ввімкнення освітлення, коли спрацює датчик руху. Більшість систем також інтегруються з іншими "розумними" пристроями, такими як розетки, термостати тощо;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		24

6) гнучкість тарифів та планів: багато хмарних систем пропонують різні плани та тарифи, що дозволяє вам вибрати той, який найбільше відповідає вашим потребам та бюджету;

7) технічна підтримка та оновлення: більшість провайдерів хмарних систем надають технічну підтримку та регулярні оновлення програмного забезпечення для підтримки безпеки та функціональності вашої системи.

Хмарні системи охоронної сигналізації є зручним та ефективним рішенням для забезпечення безпеки вашого будинку чи бізнесу, оскільки вони надають вам доступ та контроль над вашими пристроями з будь-якої точки світу.

Системи інтегрованого безпекового керування (СІБК) об'єднують в собі різні компоненти безпеки для створення комплексної та забезпеченої системи безпеки. Ось деякі ключові аспекти таких систем:

1) центральне керування: СІБК об'єднують різні системи безпеки, такі як охоронна сигналізація, відеоспостереження, контроль доступу, димові детектори тощо, під одним керівництвом. Це дозволяє централізовано контролювати та керувати всіма аспектами безпеки;

2) інтеграція пристроїв: СІБК можуть інтегрувати різні пристрої та системи, незалежно від виробника, забезпечуючи сумісність та злагоджену роботу між ними;

3) автоматизація процесів: системи інтегрованого керування можуть автоматизувати різні процеси безпеки. Наприклад, вони можуть автоматично включати відеоспостереження та активувати сигналізацію при спрацюванні датчика руху;

4) аналітика даних: СІБК можуть використовувати аналітичні інструменти для аналізу даних, збираючи інформацію з різних джерел і використовуючи її для виявлення відхилень та покращення безпеки;

5) віддалений доступ та моніторинг: власники можуть отримувати доступ до системи через Інтернет, щоб контролювати та моніторити безпеку будь-де з будь-якого пристрою;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		25

6) управління ресурсами: СІБК можуть ефективно керувати ресурсами, такими як освітлення та опалення, забезпечуючи енергоефективність та безпеку одночасно;

7) системи виявлення і превентивні заходи: вони можуть виявляти потенційні загрози та негайно реагувати на них, запобігаючи можливим інцидентам;

8) швидке реагування: СІБК надають можливість швидко реагувати на будь-які загрози або інциденти, забезпечуючи безпеку персоналу та майна.

Загалом, системи інтегрованого безпекового керування є потужними інструментами, які забезпечують комплексний захист будівель та об'єктів, підвищуючи рівень безпеки та зручності управління.

### **1.2.2 Оцінка переваг та недоліків існуючих систем**

Зважаючи на різноманіття систем безпеки, оцінка їх переваг та недоліків може допомогти вибрати найбільш підходящий варіант для конкретних потреб.

Ось загальна оцінка, яка свідчить про переваги:

1) безпека та захист: всі системи надають рівень безпеки, забезпечуючи захист від несанкціонованого доступу, виявлення пожеж та інших небезпечних ситуацій;

2) моніторинг у реальному часі: більшість систем дозволяють відстежувати події в реальному часі, що дозволяє оперативно реагувати на них;

3) віддалений доступ: багато систем пропонують можливість віддаленого керування та моніторингу через Інтернет, що дозволяє контролювати безпеку з будь-якої точки;

4) інтеграція з іншими пристроями: багато систем можуть бути інтегровані з іншими "розумними" пристроями для автоматизації різних аспектів життя;

5) легкість встановлення: бездротові системи та системи, які працюють в хмарі, зазвичай легше встановлювати, оскільки не потребують прокладання кабелів.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		26

Безпека та захист є однією з основних переваг будь-якої системи безпеки. Ось деякі аспекти, які підтверджують це:

1) виявлення вторгнень: системи безпеки, такі як системи охоронної сигналізації та відеоспостереження, дозволяють виявляти незаконний доступ або вторгнення в приміщення;

2) попередження пожеж: деякі системи включають в себе датчики диму та тепла, які негайно спрацьовують та надсилають сигнали про пожежу в разі виявлення диму або підвищеної температури;

3) доступ контролю: системи контролю доступу забезпечують захист від несанкціонованого входу в приміщення, обмежуючи доступ лише до авторизованих осіб;

4) моніторинг приміщень: відеоспостереження дозволяє в реальному часі відстежувати та контролювати дії в приміщенні, що допомагає вчасно реагувати на будь-які небезпечні ситуації;

5) датчики витоку газу та води: деякі системи безпеки включають в себе датчики витоку газу або води, які спрацьовують у разі виявлення небезпеки і надсилають сповіщення;

6) повідомлення про надзвичайні ситуації: всі ці системи можуть надсилати сповіщення про надзвичайні ситуації або тривоги на вказані контактні номери, щоб оперативно повідомити про проблеми;

7) збереження записів: системи відеоспостереження зазвичай зберігають записи про відбуті події, що може бути корисним для подальшого розслідування або аналізу.

Загалом, системи безпеки дійсно забезпечують високий рівень захисту та безпеки, забезпечуючи моніторинг, виявлення та реагування на потенційні загрози або небезпечні ситуації.

Можливість моніторингу у реальному часі є важливою функцією більшості систем безпеки. Ось деякі переваги цієї можливості:

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		27

1) швидка реакція на події: завдяки моніторингу у реальному часі ви можете швидко реагувати на будь-які події чи небезпечні ситуації, які виникають в приміщенні;

2) оперативне повідомлення: системи надсилають сповіщення в реальному часі про будь-які події або тривоги, що дозволяє оперативно реагувати на них;

3) віддалений моніторинг: багато систем дозволяють віддалено моніторити події, що сталося в приміщенні, через мобільні додатки або веб-портали, навіть якщо ви не знаходитесь на місці;

4) виявлення небезпеки: моніторинг у реальному часі дозволяє вчасно виявляти небезпеку, таку як вторгнення, пожежа чи витік газу, і вживати відповідні заходи для захисту;

5) подальший аналіз та розслідування: записи про події у реальному часі можуть бути збережені для подальшого аналізу чи розслідування інцидентів;

6) контроль працівників: моніторинг у реальному часі дозволяє відстежувати дії працівників на робочому місці, що може покращити безпеку та ефективність роботи;

7) покращення реагування на аварії: миттєве виявлення аварійних ситуацій дозволяє вжити негайних заходів для запобігання та мінімізації можливих збитків.

Усі ці аспекти роблять моніторинг у реальному часі надзвичайно важливою функцією для ефективною системи безпеки, дозволяючи оперативно реагувати на потенційні загрози та забезпечуючи безпеку приміщення.

Можливість віддаленого доступу є дуже корисною функцією для систем безпеки. Ось деякі переваги цієї можливості:

1) гнучкість: можна контролювати та моніторити свою систему безпеки з будь-якого місця, де є доступ до Інтернету. Це може бути корисно як вдома, так і поза її межами, наприклад, у відпустці або в подорожі;

2) відстеження статусу системи: можна перевіряти статус системи в будь-який час, щоб переконатися, що всі компоненти працюють належним чином і що немає тривожних ситуацій;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>28</b>

3) віддалене керування: можна керувати різними аспектами системи безпеки, такими як активація або деактивація сигналізації, ввімкнення та вимкнення відеоспостереження, а також керування іншими функціями, які можуть бути доступні;

4) віддалені сповіщення: можна отримувати сповіщення про будь-які події або тривоги на ваш мобільний телефон або інший пристрій, навіть якщо ви не знаходитесь в будинку чи на роботі;

5) віддалене ведення журналу: деякі системи зберігають журнали подій, які можна переглядати віддалено, що дозволяє вам перевіряти, що відбувається під час вашої відсутності;

6) ефективне управління віддалено: ви можете ефективно керувати системою, навіть якщо видалені від неї. Це дозволяє вам реагувати на будь-які ситуації та контролювати безпеку свого приміщення, навіть коли ви не знаходитесь поруч.

Ці можливості роблять віддалений доступ надзвичайно корисним для забезпечення безпеки та контролю над вашим приміщенням у будь-який час та з будь-якого місця.

Легкість встановлення є важливою перевагою бездротових систем та систем, які працюють в хмарі. Ось деякі аспекти, які підтверджують цю перевагу:

1) відсутність необхідності в кабелях: бездротові системи та системи, які працюють в хмарі, не потребують прокладання кабелів для підключення компонентів. Це робить процес встановлення значно швидшим та менш проблематичним;

2) менше обмежень монтажу: бездротові пристрої можна встановлювати в місцях, де прокладання кабелів було б важко або неможливо, таких як стелі, стіни або вікна;

3) менше пошкоджень і будівельних робіт: відсутність кабелів означає менше пошкоджень стін, підлоги чи стелі під час встановлення. Це зменшує витрати на ремонт та робочу силу;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>29</b>

4) можливість швидкого переміщення: бездротові пристрої легко переміщувати з одного місця в інше без необхідності перекладання кабелів;

5) зменшення витрат на інфраструктуру: не потрібно витрачати кошти на закупівлю та встановлення дорогих кабелів та аксесуарів для їх монтажу;

6) простота самостійного встановлення: багато бездротових систем призначені для самостійного встановлення користувачами, що зменшує потребу у фахівцях з монтажу та зберігає час та гроші;

7) легка масштабованість системи: додавання нових компонентів до бездротової системи зазвичай дуже просте, що дозволяє швидко розширювати функціональність та покриття системи.

У цілому, легкість встановлення є важливою перевагою бездротових систем та систем, які працюють в хмарі, спрощуючи процес установки та забезпечуючи більшу гнучкість у виборі місць розташування пристроїв.

До недоліки можна віднести наступне:

1) вартість: деякі системи можуть бути високою за вартістю, особливо якщо вони мають багато функцій або використовують передові технології;

2) залежність від Інтернету: хмарні системи потребують постійного з'єднання з Інтернетом, тому в разі відключення мережі може бути обмежений доступ або функціональність;

3) можливість взлому: жодна система не є абсолютно непроникною, існує ризик, що деякі системи можуть бути взломані або обійдені;

4) потреба у технічній підтримці: деякі системи можуть вимагати налаштування та технічної підтримки, що може бути складним для користувача без відповідних навичок;

5) приватність даних: використання систем, які зберігають дані в хмарі, може ставити питання щодо приватності та безпеки цих даних;

6) потреба в електропостачанні: безпекові системи потребують стабільного джерела живлення, тому можуть бути вразливі до перерв у електропостачанні.

Обираючи систему безпеки, важливо враховувати специфічні потреби та обставини, а також балансувати переваги та недоліки різних варіантів.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		30

### 1.2.3 Аналіз вимог до системи охорони периметру об'єкту

Аналіз вимог до системи охорони периметру об'єкту важливий для ефективного захисту території. Ось деякі аспекти, які слід врахувати при аналізі вимог:

1) розмір та форма об'єкту: розмір і форма об'єкту визначають кількість та розташування необхідних датчиків і камер, а також типи перешкод, які можуть бути використані для охорони;

2) природні перешкоди: природні перешкоди, такі як річки, ліси чи гори, можуть створювати природний бар'єр для неповного оточення об'єкту;

3) інфраструктура об'єкту: будівлі, дороги, паркани та інші елементи інфраструктури об'єкту впливають на вибір технологій та місць встановлення обладнання;

4) стратегічні точки входу та виходу: важливо визначити головні точки входу та виходу, а також можливі шляхи, які можуть використовуватися для незаконного проникнення на територію;

5) типи загроз: враховуючи потенційні загрози, такі як вторгнення людей, злочинців чи терористичні акти, слід визначити, які заходи безпеки є найбільш ефективними;

6) відстань до сусідів та загальний рівень безпеки в районі: це може впливати на вимоги до системи охорони та на рішення про використання додаткових заходів безпеки;

7) необхідність інтеграції з іншими системами безпеки: якщо на об'єкті вже використовуються інші системи безпеки (наприклад, системи контролю доступу або системи відеоспостереження), важливо забезпечити їх сумісність та інтеграцію;

8) бюджет: від визначення бюджету залежить вибір оптимального рішення, враховуючи витрати на обладнання, монтаж та підтримку системи.

На основі аналізу цих факторів можна розробити оптимальний план системи охорони периметру, який відповідатиме потребам та умовам конкретного об'єкту.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>31</b>

## 1.3 Проектування системи охоронної сигналізації офісу

### 1.3.1 Вибір технічних засобів системи

Проектування системи охоронної сигналізації для офісу – це важливий процес, який має захищати працівників, обладнання та конфіденційну інформацію. Ось кроки, які слід виконати при проектуванні такої системи:

1) аналіз вимог та загроз:

- потрібно визначити типи загроз, з якими може стикнутися офіс (наприклад, злам системи, крадіжки, пожежі тощо);

- потрібно встановити вимоги до системи охоронної сигналізації, враховуючи розмір та масштаб офісу, кількість працівників та рівень доступу;

2) планування розміщення датчиків та камер:

- потрібно визначити оптимальні місця для розташування датчиків руху, датчиків диму, контактних датчиків та камер в зоні входів, коридорів, кімнат та інших важливих зон офісу;

- потрібно розглянути можливі місця для розміщення пульта керування та індикаторів тривоги;

3) вибір системи сигналізації:

- потрібно вибрати тип системи сигналізації (дротова, бездротова або гібридна) в залежності від вимог та можливостей офісу;

- потрібно розглянути системи, які включають в себе додаткові функції, такі як контроль доступу, відеоспостереження та автоматичне сповіщення;

4) інтеграція з іншими системами безпеки:

- необхідно забезпечити інтеграцію системи охоронної сигналізації з іншими системами безпеки, такими як системи відеоспостереження та контролю доступу;

5) розробка процедур реагування на тривоги:

- необхідно розробити процедури для випадків спрацювання тривоги: хто і як буде реагувати на сигнали тривоги, які кроки слід вжити тощо;

6) вибір обладнання та програмування:

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		32

- необхідно вибрати обладнання, яке найкраще відповідає вимогам та можливостям офісу;

- потрібно налаштувати програмне забезпечення для контролю та моніторингу системи;

7) тестування та навчання персоналу:

- потрібно провести тестування системи для переконання у її працездатності та надійності;

- необхідно навчити персонал користуватися системою та вмикати/вимикати тривоги;

8) впровадження та підтримка:

- введіть систему в експлуатацію та забезпечте постійне технічне обслуговування;

- забезпечте постійну підтримку та оновлення системи;

9) оновлення та вдосконалення:

- періодично переглядайте та оновлюйте систему, враховуючи зміни у вимогах та технологіях.

Проектування системи охоронної сигналізації для офісу має забезпечувати ефективний захист приміщення та персоналу, забезпечуючи високий рівень безпеки та комфорту.

### **1.3.2 Доцільність застосування платформи Arduino для проектування системи сигналізації офісу**

Застосування платформи Arduino для проектування системи сигналізації офісу має кілька значних переваг:

1) вартість: Arduino - це відома своєю доступністю та низькою вартістю. Для невеликих і середніх офісів це може бути особливо важливим, оскільки знижує загальні витрати на обладнання;

2) простота використання: Arduino має простий інтерфейс, який дозволяє швидко розробляти та налаштовувати систему, навіть для людей без глибоких знань програмування або електроніки;

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		33

3) гнучкість та модульність: платформа Arduino має велику кількість розширень та модулів, що дозволяє легко налаштувати систему відповідно до конкретних потреб офісу. Це дозволяє використовувати різні типи датчиків (руху, диму, газу тощо), реле, LCD дисплеї, а також здійснювати зв'язок через Wi-Fi, Bluetooth або GSM;

4) широкі можливості інтеграції: Arduino легко інтегрується з іншими системами безпеки, такими як системи відеоспостереження, контролю доступу або системи автоматизації будівель. Це забезпечує комплексний підхід до безпеки офісу;

5) велика спільнота та підтримка: Arduino має велику спільноту користувачів, що спрощує пошук інформації, вирішення проблем та обмін досвідом. Також існує велика кількість доступних бібліотек та прикладів коду, що дозволяє швидко створювати функціональні системи;

6) можливість розширення та оновлення: існують безліч проектів та модулів, які можна легко використовувати для розширення функціоналу системи. Це дозволяє оновлювати та модернізувати систему з плином часу;

Однак, слід врахувати, що Arduino має свої обмеження, особливо щодо продуктивності та безпеки даних. Для більших офісів або для проектів, де важливість надійності та безпеки вища, може бути доцільним розглядати більш потужні та професійні платформи.

У загальному, застосування платформи Arduino для проектування системи сигналізації офісу є доцільним завдяки своїм перевагам у вартості, простоті використання та гнучкості. Вона дозволяє створити ефективну та економічно вигідну систему безпеки, враховуючи конкретні потреби та обмеження офісу.

### **1.3.3 Розробка системи охорони сигналізації офісу**

Проведено аналіз приміщень офісу, в яких є вікна та двері. На рис. 1.9 наведено план офісу, який має чотири кімнати, хол, санітарну кімнату і кімнату охоронника. Проведено аналіз з точки зору розміщення датчиків охоронної сигналізації:

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		34

1) кімната директор має площу 15 кв м та одне вікно. Небезпекою для цього приміщення є вікно, через яке зловмисник може проникнути, тому доцільно розмістити на цьому вікні магнітоконтатний датчик (геркон), який спрацює на відкриття;

2) кімната секретарки має площу 15 кв м та одне вікно. В цій кімнаті також доцільно розмістити на вікні магнітний датчик на відкриття;

3) кімната постачання та збуту має площу 30 кв м та одне вікно. В цій кімнаті розмістимо на вікні магнітоконтатний датчик на відкриття;

4) кімната охоронника має площу 15 кв м та одне вікно, для якого доцільно встановити магнітоконтатний датчик та пульт керування системою сигналізації, блок аварійного живлення, комп'ютер або доцільно включити ноутбук, що дасть можливість продовжувати безперебійну роботи у випадку відключення живлення.



Рисунок 1.9. План офісу для розміщення системи сигналізації

### 1.3.4 Цифровий модуль датчика нахилу

Digital Tilt Senso від RobotDyn – це цифровий модуль датчика нахилу, який працює на простому, але ефективному принципі. Основним компонентом цього модуля є датчик нахилу або акселерометр.

Принцип роботи полягає у вимірюванні прискорення, з якого можна визначити нахил відносно земної поверхні. Акселерометр виявляє зміни в гравітаційному полі, які виникають від нахилу модуля. За допомогою цих змін датчик визначає кут нахилу відносно горизонту. На платі є герметична скляна колба з двома контактами та металевою кулькою. При нахилі кулька перекочується і замикає контакт, при нахилі в інший бік розмикає ланцюг. Має багато застосувань, де важливо враховувати орієнтацію у просторі. Наприклад, можна використовувати як простий перемикач при нахилі.

Цифровий модуль Digital Tilt Senso має вбудований аналогово-цифровий перетворювач (ADC), який перетворює сигнали з датчика на цифрові дані, зрозумілі для мікроконтролера. Це дозволяє зручно і швидко отримувати дані про нахил через цифровий інтерфейс.

Всі ці дані можуть використовуватися для контролю рухомих систем, стабілізації об'єктів, регулювання напрямку, автоматизації рухомих платформ та багатьох інших застосувань, де необхідно вимірювати нахил.

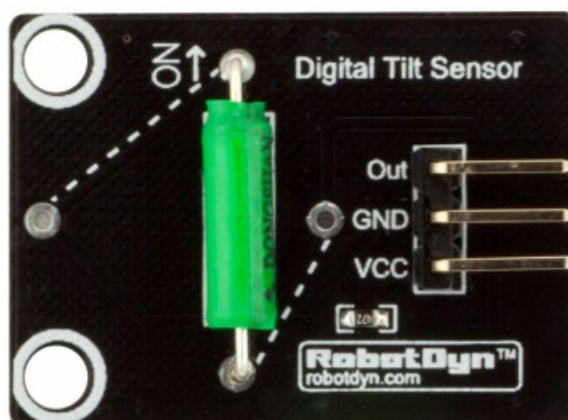


Рисунок 1.10. Цифровий модуль Digital Tilt Senso

Digital Tilt Senso має декілька переваг, які роблять його привабливим для використання:

1) простота використання: модуль простий у встановленні і використанні. Його можна підключити безпосередньо до мікроконтролера або одноплатного комп'ютера, що робить процес інтеграції дуже простим;

2) висока точність: акселерометр в цьому модулі зазвичай має дуже високу точність, що дозволяє отримувати точні дані про нахил;

3) цифровий інтерфейс: модуль працює за допомогою цифрового інтерфейсу, що робить його сумісним з більшістю мікроконтролерів та одноплатних комп'ютерів. Це спрощує обробку даних і взаємодію з модулем;

4) малий розмір: модуль має компактні розміри, що дозволяє легко вбудовувати його в різні пристрої та конструкції без значного збільшення їх розмірів;

5) низька вартість: Digital Tilt Senso відносно недорогий, що робить його доступним для широкого кола розробників та хобістів;

6) різноманітність застосувань: модуль може бути використаний в різних застосуваннях, від контролю рухомих систем до стабілізації камер або платформ, від автомобільної електроніки до іграшок та роботів.

Ці переваги роблять Digital Tilt Senso привабливим вибором для тих, хто шукає надійний та доступний датчик нахилу для своїх проектів.

На рис. 1.11 надано розміщення датчиків нахилу Digital Tilt Senso в системі охоронної сигналізації офісу. Датчики нахилу Digital Tilt Senso позначені на схемі TILT1 ... TILT6 та розміщуються на кожне вікно приміщення офісу.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		37

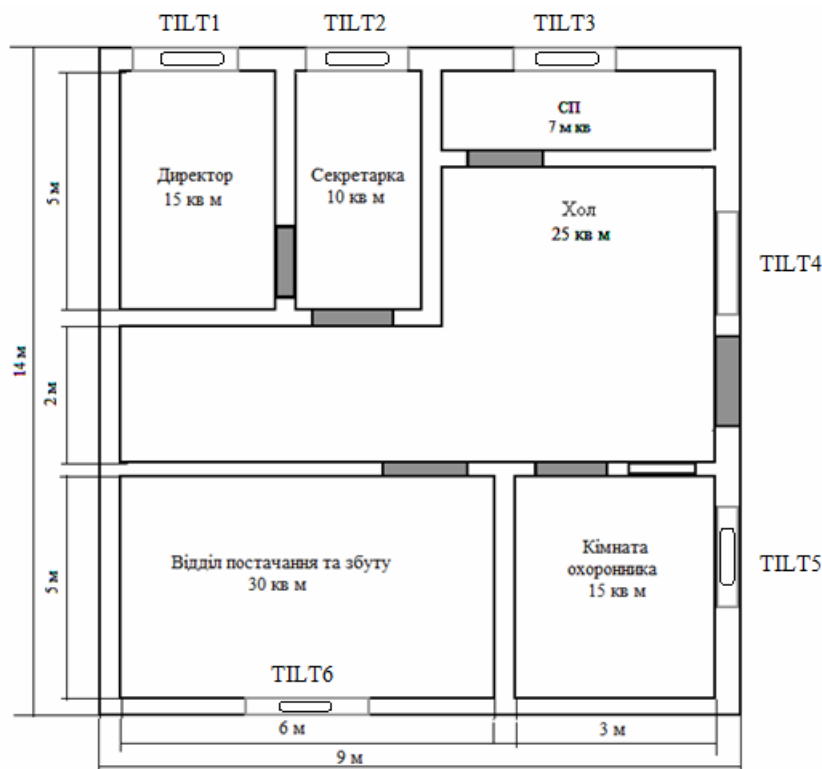


Рисунок 1.11. Розміщення датчиків нахилу в системі Digital Tilt Senso охоронної сигналізації офісу

### 1.3.5 Розробка схеми електричної принципіальної системи охоронної сигналізації

Для розробки схеми електричної принципіальної системи охоронної сигналізації було використано симулятор Arduino. Це дало змогу спочатку перевірити працездатність схеми.

Симулятор Arduino – це інструмент, який дозволяє розробникам програмного забезпечення для платформи Arduino виконувати та тестувати свій код без фактичного апаратного з'єднання з мікроконтролером. Такий інструмент забезпечує ряд можливостей:

1) віртуальна плата Arduino: симулятор надає можливість використовувати віртуальну плату Arduino, яка імітує реальну плату, включаючи мікроконтролер та його периферійні пристрої;

2) виконання коду без реальної плати: розробники можуть завантажити свій код у симулятор Arduino і виконувати його без прив'язки до фізичної плати.

Це дозволяє швидко тестувати програми без необхідності кожного разу використовувати реальне обладнання;

3) симуляція введення/виведення: симулятор надає можливість імітувати введення (наприклад, сигнали від датчиків або кнопок) та виведення (наприклад, сигнали до світлодіодів або інших пристроїв) для тестування взаємодії програми з реальними введення та виведення;

4) візуалізація даних: симулятор може візуалізувати дані, що виводяться, що дозволяє розробникам відстежувати стан внутрішніх змінних або сигналів під час виконання програми;

5) налаштування середовища: деякі симулятори дозволяють налаштовувати параметри середовища, такі як розмір пам'яті, роботу таймерів, наявність певних пристроїв і т. д., що дозволяє виконувати більш реалістичні тестування;

6) навчальні матеріали: багато симуляторів мають навчальні матеріали або документацію, яка допомагає новачкам ознайомитися з платформою Arduino та програмуванням для неї.

Загалом, симулятор Arduino спрощує розробку та тестування програмного забезпечення для платформи Arduino, зменшуючи залежність від фізичного обладнання і полегшуючи процес відлагодження.

На рис. 1.12 надана візуалізація схеми пристроїв системи охоронної сигналізації офісу на основі симулятору платформи Arduino.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		39

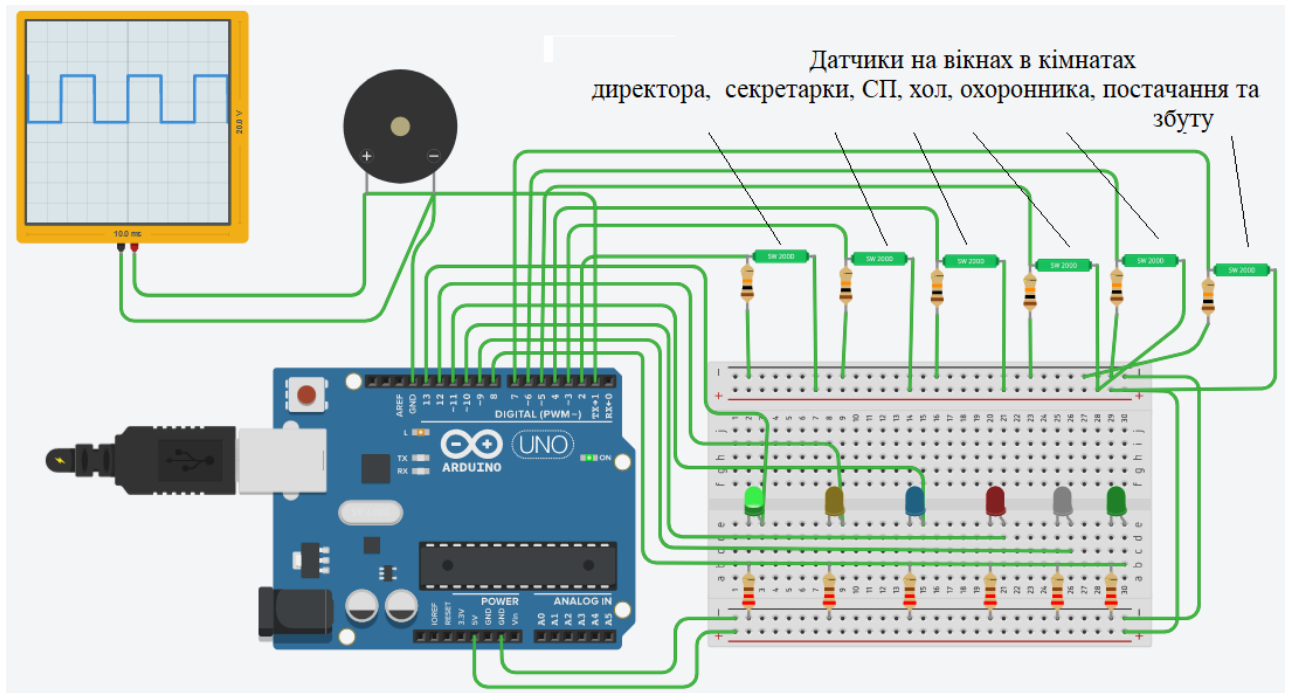


Рисунок 1.12. Візуалізація схеми пристроїв системи охоронної сигналізації офісу на основі симулятора

Для завдання налагоджувальна сигналу оповіщення було використано осцилограф. Робота в симуляторі дала можливість побудувати схему системи охоронної сигналізації офісу, розробити скетч програми, провести налагоджування та перевірити працездатність. На рис. 1.13 надана схема електрична принципальна системи охоронної сигналізації офісу. В табл. 1.1 надано перелік елементів схеми електричної принципальної

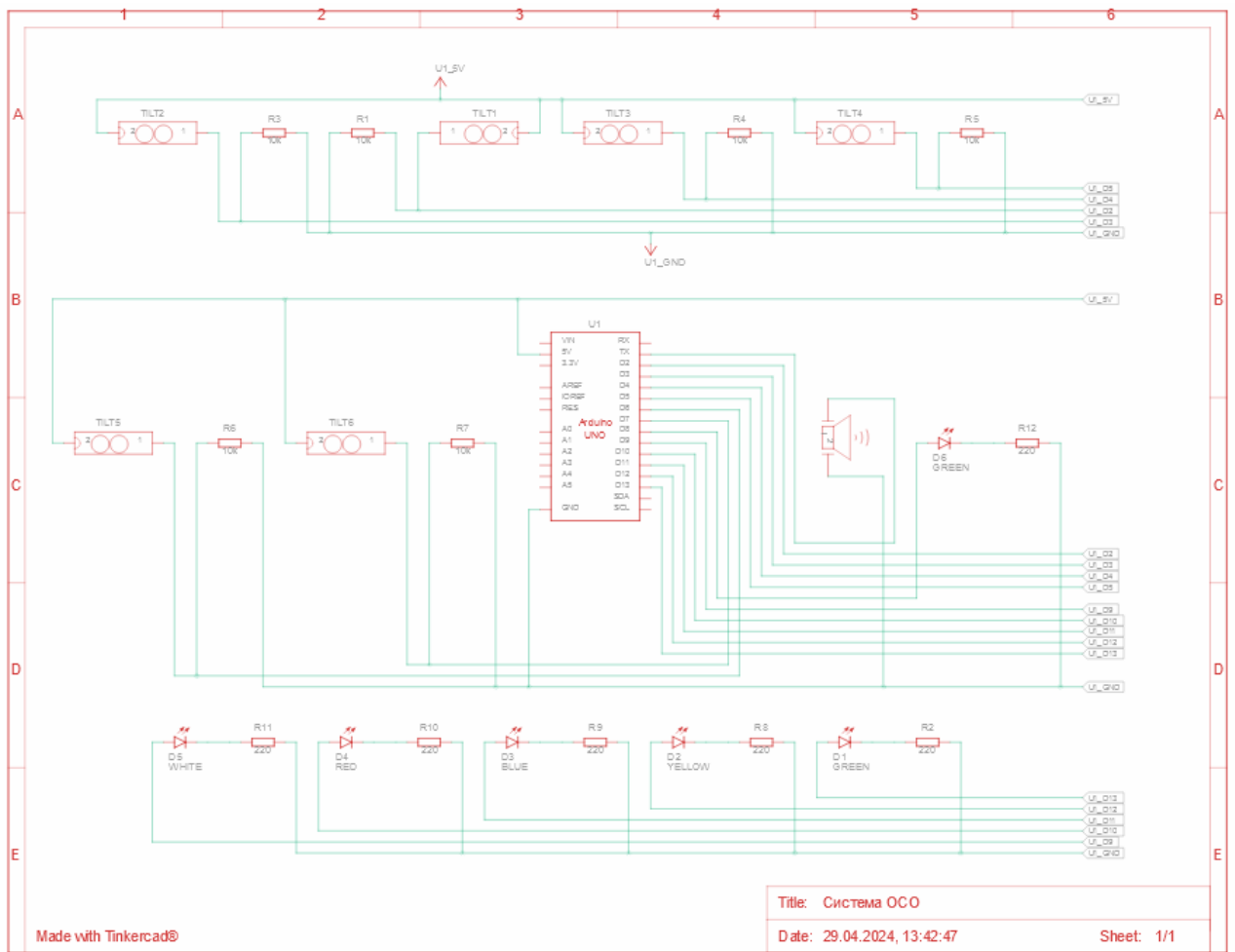


Рисунок 1.13. Схема електрична принципіальна системи охоронної сигналізації офісу

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		41

Таблиця 1.1. Перелік радіоелементів на схемі

Найменування радіоелемента на схемі	Кількість	Радіоелемент
U1	1	Arduino Uno R3
R1 R3 R4 R5 R6 R7	6	10 k $\Omega$ Resistor
TILT1 TILT2 TILT3 TILT4 TILT5 TILT6	6	Tilt Sensor
R2 R8 R9 R10 R11 R12	6	220 $\Omega$ Resistor
D1 D6	2	Green LED
D2	1	Yellow LED
D3	1	Blue LED
D4	1	Red LED
D5	1	White LED
PIEZO1	1	Piezo
B	1	Вимикач системи сигналізації

### 1.3.6 Розробка програмного забезпечення системи охоронної сигналізації

Розробка програмного забезпечення для платформи Arduino включає кілька етапів:

1) встановлення середовища розробки (IDE): першим кроком є встановлення Arduino IDE (інтегроване середовище розробки) на ваш комп'ютер.

Це безкоштовне програмне забезпечення, яке дозволяє писати, компілювати та завантажувати код на плату Arduino;

2) вибір плати та налаштування середовища: у Arduino IDE вибираєте тип плати, яку ви використовуєте (наприклад, Arduino Uno, Nano, Mega і т. д.). Також налаштовуєте COM-порт, який використовується для зв'язку з Arduino;

3) створення скетча (програми): У Arduino IDE створюєте новий скетч (програму) або відкриваєте існуючий. Arduino-програми складаються з функцій `setup()` (ініціалізація) та `loop()` (головний цикл). У функції `setup()` ви визначаєте початкові налаштування, а в функції `loop()` розміщується основний код, який виконується постійно;

4) написання коду: потрібно написати код для виконання певних завдань. Це може бути керування світлодіодами, робота з сенсорами, взаємодія з іншими пристроями тощо. Arduino використовує мову програмування C/C++, але зі спеціальними функціями та бібліотеками, що спрощують взаємодію з обладнанням;

5) компіляція коду: після написання коду ви компілюєте його в Arduino IDE. Компіляція перевіряє синтаксичну правильність коду і перетворює його в машинний код, який може виконуватися на мікроконтролері Arduino;

6) завантаження коду на плату: після успішної компіляції ви завантажуєте скомпільований код на плату Arduino через USB-порт. Arduino IDE автоматично визначає, яка плата підключена і який COM-порт використовується;

7) відлагодження (дебагінг): Якщо код не працює так, як очікувалося, можна використовувати серійний монітор у Arduino IDE для виведення додаткової інформації про поточний стан програми та її змінні;

8) тестування та вдосконалення: після завантаження програми на плату Arduino ви можете провести тестування її роботи. Якщо є помилки або несправності, ви виправляєте їх у коді та повторюєте процес;

9) документація: не забувайте добре документувати ваш код, описуючи, що робить кожна частина програми та як вона працює. Це полегшить розуміння вашого коду і допоможе іншим розробникам або вам самим у майбутньому.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		43

Цей процес дозволяє створювати різноманітні проекти для платформи Arduino, від простих світлодіодних маячків до складних автоматизованих систем керування. Розглянемо складові розробленого скетча, який складається з трьох частин. В першій частині змінним `buttonState2 ... buttonState7` встановлюється початковий рівень нуль.

У другій частині програми `void setup()` відбувається програмування портів за допомогою, наприклад, команд `pinMode(2, INPUT)` та `pinMode(13, OUTPUT)`: порт №2 є входом; порт №13 є виходом.

У третій частині програми `void loop()` спочатку за допомогою команди `digitalRead( )` записується в `buttonState2 ... buttonState2` стан датчиків системи охоронної сигналізації. Далі за допомогою оператора `if – else` відбувається перевірка станів датчиків. За умови, що датчик спрацював загоряється відповідний світлодіод та звучить звуковий сигнал тривоги. Для кожного приміщення передбачено свій світлодіод та певна частота звучання.

```
int buttonState2 = 0; // встановлюється початковий рівень нуль – кабінет
директора
int buttonState3 = 0; // кабінет секретарки
int buttonState4 = 0; // санітарне приміщення
int buttonState5 = 0; // хол
int buttonState6 = 0; // кабінет охоронника
int buttonState7 = 0; // кабінет постачальника та збуту
void setup()
{
  pinMode(2, INPUT); // порт 2 встановлюються вхідним для датчика
нахилу – вікно кабінету директора
  pinMode(13, OUTPUT); // порт 13 встановлюються вихідним – світлодіод
для сигналізації кабінету директора
  pinMode(3, INPUT); // ... кабінет секретарки
  pinMode(12, OUTPUT); // ... кабінет секретарки
```

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		44

```

pinMode(4, INPUT); // ... санітарне приміщення
pinMode(11, OUTPUT); // ... санітарне приміщення
pinMode(5, INPUT); // ... хол
pinMode(10, OUTPUT); // ... хол
pinMode(6, INPUT); // ... кабінет охоронника
pinMode(9, OUTPUT); // ... кабінет охоронника
pinMode(7, INPUT); // ... кабінет постачальника та збуту
pinMode(8, OUTPUT); // ... кабінет постачальника та збуту
}

void loop()
{
    // фіксація станів датчиків нахилу в приміщеннях
    buttonState2 = digitalRead(2);
    buttonState3 = digitalRead(3);
    buttonState4 = digitalRead(4);
    buttonState5 = digitalRead(5);
    buttonState6 = digitalRead(6);
    buttonState7 = digitalRead(7);

    // перевірка станів датчиків нахилу
    if (buttonState2 == HIGH) {
        // turn LED on
        digitalWrite(13, HIGH);
        tone(1,300,500); // формування звукового сигналу з частотою 300 Гц
        тривалістю 500 мілісекунд при спрацьовуванні сигналізації в кабінеті директора
    } else {
        // turn LED off
        digitalWrite(13, LOW);
    }
    delay(10); // затримка на 11 мілі секунд
    if (buttonState3 == HIGH) {

```

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		45

```

// turn LED on
digitalWrite(12, HIGH);
tone(1,500,500);
} else {
// turn LED off
digitalWrite(12, LOW);
}
delay(10); //
if (buttonState4 == HIGH) {
// turn LED on
digitalWrite(11, HIGH);
tone(1,700,500); //
} else {
// turn LED off
digitalWrite(11, LOW);
}
delay(10); //
if (buttonState5 == HIGH) {
// turn LED on
digitalWrite(10, HIGH);
tone(1,900,500);
} else {
// turn LED off
digitalWrite(10, LOW);
}
delay(10); //
if (buttonState6 == HIGH) {
// turn LED on
digitalWrite(9, HIGH);
tone(1,1100,500);

```

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
						<b>46</b>
Зм.	Арк.	№ докум.	Підпис	Дата		

```
} else {  
    // turn LED off  
    digitalWrite(9, LOW);  
}  
delay(10); //  
if (buttonState7 == HIGH) {  
    // turn LED on  
    digitalWrite(8, HIGH);  
    tone(1,1200,500);  
} else {  
    // turn LED off  
    digitalWrite(8, LOW);  
}  
delay(10); //
```

					КС 57. 19 000. 00 ДП ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		47

## 2 ЕКОНОМІЧНИЙ РОЗДІЛ

### 2.1 Резюме

Темою даного дипломного проекту є озробка системи охоронної сигналізації офісу. В дипломній роботі створена система охоронної сигналізації офісу із застосуванням платформи Arduino. Для завдання розробки обрано датчик нахилу, який розміщується на вікна приміщень офісу.

Ефективність кожного програмного продукту визначається його якістю та ефективністю процесу розробки. Якість ПП визначається наступними складовими: з точки зору користувача; з позиції використання ресурсів; виконання вимог до програмного забезпечення.

Проведемо розрахунки визначення трудомісткості розробки даного програмного продукту.

### 2.2 Розрахунок ціни програмного продукту нормативним методом

#### 2.2.1 Визначення трудомісткості розробки програмного забезпечення

Тривалість розробки програмного продукту залежить від його обсягу, трудомісткості розробки, кваліфікації виконавців, а також планових термінів, визначених умовами ринку.

У табл. 2.1 представлені аналоги програмного забезпечення, функції яких, у більшому або меншому ступені, виконує розроблений програмний продукт.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
						<b>48</b>
Зм.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1 – Каталог аналогів

Найменування ПП	Обсяг функції ПП – $V_o$ , усл. машинних командах.
1. ПП СУБД	2500 – 9800
2. Комплексні системи ведення БД	950 – 7430
3. ПП введення інформації	1060 – 5750
4. ПП оптимізації розрахунків	1300 – 4200
5. ПП автоматизації засобів по каталогу	680 – 7000
6. ПП автоматизованих розрахунків	1300 – 8600
7. ПП загальної математики і ПП імітаційного моделювання	7800 – 8800
8. ПП організації обчислювального процесу	13000 – 10200

Для нашого варіанта виділено сірим кольором.

Вибравши аналог ПП, що містить  $V_o$  в умовних машинних командах, трудомісткості визначати на основі табл.2.2.

Таблиця 2.2 –Трудомісткість

Обсяг ПП, тис.умов.машинних команд	Норма часу, люд/год
1.00	229
2.00	244
3.00	262
4.00	283

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера,  $K_k=0,7\div 0,8$ ):  $T_{ар} = 229 \times 0,8 = 183,2$  (люд/годин).

Трудомісткість програмного продукту визначається по кожному етапу розробки окремо на підставі трудомісткості аналога з урахуванням складності розробки, ступеня новизни і ступеня використання в розробці стандартних модулів на підставі формул:

$$T_{ТЗ} = T^a p \times L_1 \times K_H \quad (2.1)$$

$$T_{ТП} = T^a p \times L_2 \times K_H \quad (2.2)$$

$$T_{РП} = T^a p \times L_3 \times K_H \times K_T \quad (2.3)$$

Для розрахунку необхідні наступні коефіцієнти:

$L_i$  – питома вага  $i$ -го етапу розробки (див. табл. 2.2.);

$K_H$  – поправочний коефіцієнт, що враховує ступінь новизни (див. табл. 2.3.);

$K_T$  – поправочний коефіцієнт, що враховує ступінь використання в розробці типових програм (див. табл. 2.4.).

Таблиця 2.3 – Значення питомих коефіцієнтів трудомісткості стадії в загальній трудомісткості розробки ПП

Код стадії	Ступінь новизни		
	А	Б	В
ТЗ ( $L_1$ )	0,15	0,12	0,12
ТП ( $L_2$ )	0,16	0,15	0,11
РП ( $L_3$ )	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4 – Значення поправочного коефіцієнта, що враховує ступінь новизни

Код ступеня новизни	Ступінь новизни	Значення $K_H$
А	Принципово нові ПП	1,75 – 1,2
Б	ПП – розвиток визначеного параметричного ряду	1,0 – 0,8
В	ПП маючий аналог	0,7

Для нашого варіанта виділено сірим кольором.

Тому що розробка системи є ПП, що має аналоги програмних продуктів, то код ступеня новизни для мого ПП – В, а значення коефіцієнта  $K_H=0,7$ . По таблиці 2.5, знаючи код ступеня новизни, тепер можна визначити значення питомих коефіцієнтів трудомісткості:  $L_1=0,12; L_2=0,11; L_3=0,61$ ;

Таблиця 2.5 – Значення коефіцієнта ступеня використання в розробці типових програм

Ступінь охоплення реалізованих функцій розроблювального ПП типовими програмами, %	Значення $K_T$
60 і вище	0,6
40-60	0,7
20-40	0,8
До 20	0,9

Для нашого варіанта виділено сірим кольором.

У розробленому програмному продукті використовується від 40 до 60 відсотків існуючих функцій, це значить, що  $K_T=0,7$ .

Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$T_{ТЗ}=T_a * L_1 * K_H = 183,2 * 0,12 * 0,7 = 15,39 \text{ (люд/годин)} \quad (2.4)$$

Трудомісткість розробки технічного проекту

$$T_{ТП}=T_a * L_2 * K_H = 183,2 * 0,11 * 0,7 = 17,42 \text{ (люд/годин)} \quad (2.5)$$

## Трудомісткість розробки робочого проекту

$$T_{\text{рп}} = T_a * L_3 * K_n * K_t = 183,2 * 0,61 * 0,7 * 0,7 = 54,76 \text{ (люд/годин)} \quad (2.6)$$

Для подальших розрахунків визначили кількість папера, витраченого на кожен етап: - технічне завдання  $N_{\text{ТЗ}}=2$  (стр), - розробка ТП  $N_{\text{ТП}}=28$ (стр), - розробка робочого проекту  $N_{\text{рп}}=37$  (стр), - пояснювальна записка відповідно  $N_{\text{пз}}=30$  (стр)

Розрахунок зведений у табл. 2.6.

### 2.2.2 Розрахунок ціни програмного продукту

У цьому розділі для визначення ціни розраховуємо основну заробітну плату виконавців, матеріальні витрати, вартість машино – години і витрати на розробку ПП. Розрахунок основної заробітної плати виконавців приведений у таблиці 2.7. Відповідно до статті 8 «Закону про Державний бюджет України на 2024» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2024 року - 8000 гривень; мінімальну погодинну тарифну ставку – 48.10 грн.

Таблиця 2.6 – Розрахунок трудомісткості ПП

Найменування етапів	Розрахунок, годин.		
	2	3	4
1.ТЗ	$T_{\text{РТЗ}}=15,39$	$T_{\text{кк}}=0,7*N_{\text{ТЗ}}=0,7*2=1,4$	$T_{\text{нк}}=0,15*N_{\text{ТЗ}}=0,15*2=0,30$
2.Розробка ТП	$T_{\text{РТП}}=14,12$	$T_{\text{кк}}=0,7*N_{\text{ТП}}=0,7*28=19,6$	$T_{\text{нк}}=0,15*N_{\text{ТП}}=0,15*28=4,2$
3.Розробка РП	$T_{\text{Ррп}}=54,76$	$T_{\text{кк}}=0,7*N_{\text{рп}}=0,7*37=25,9$	$T_{\text{нк}}=0,15*N_{\text{рп}}=0,15*37=5,55$
4.Розробка ПЗ	$T_{\text{пз}}=1,5**N_{\text{пз}}=1,5*30=45$	$T_{\text{кк}}=0,7*N_{\text{ТЗ}}=0,7*30=21$	$T_{\text{нк}}=0,15*N_{\text{пз}}=0,15*30=4,5$
Усього, в т.ч.:	231,56		
- на розробку	$\Sigma T_p=149,11$		

- контроль керівника		$\Sigma T_{\text{кк}}=67,8$	
- нормоконтроль			$\Sigma T_{\text{нк}}=14,55$

Таблиця 2.7 – Розрахунок основної заробітної плати виконавців

Найменування робіт	Трудомісткість робіт, години	Погодинна тарифна ставка, грн.	Розрахунок, грн.
1.Розробка ПП	149,11	48.10	5384,36
2.Контроль керівника	67,8	48.10	2583,18
3.Нормоконтроль	14,55	48.10	554,36
Усього	-	-	$\Sigma Z_0= 8521,90$

Зробимо розрахунок матеріальних витрат на розробку ПП. Розрахунок зведемо в табл. 2.8.

Таблиця 2.8 – Розрахунок матеріальних витрат на розробку ПЗ

Найменування матеріальних витрат	Тип, модель	Кількість	Ціна одиниці, грн.	Вартість, грн.
Папір	Лист А4	100	1.5	150,0
Папір	Лист А1	4	15,0	60,0
Разом	-	-	-	$V_{\text{мі}}=210,0$
Транспортно – заготівельні Витрати (10%)				$V_{\text{тр}_z} = 0,1 \times V_{\text{мі}} = 0,1 \times 210 = 21,0$
Усього				$V_{\text{м}} = V_{\text{мі}} + V_{\text{тр}_z} = 231.0$

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		53

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому ПП за формою, приведеною в табл. 2.9.

Таблиця 2.9 – Розрахунок статей витрат планової собівартості

Стаття витрат	Значення, грн.	Формула розрахунку
1. Матеріали	231,0	$V_M$ (див. табл. 2.7)
2. Основна заробітна плата	8521,90	$Z_o$ (див. табл. 2.6)
3. Додаткова заробітна плата	852,19	$Z_d = 0,1 \times Z_o = 8521,90 \times 0,1$
4. Відрахування до єдиного фонду соціального внеску	2062,30	$V_{\text{с.в.}} = 0,22 \times (Z_o + Z_d) = 0,22 \times (8521,90 + 852,19)$
5. Накладні витрати	3408,76	$V_{\text{нак.}} = 0,4 \times Z_o = 0,4 \times 8521,90$
6. Повна собівартість	15076,15	$C_{\text{пов}} = V_M + Z_o + Z_d + V_{\text{с.в.}} + V_{\text{нак.}} = 231,0 + 8521,90 + 852,19 + 2062,30 + 3408,76$

Розмір прибутку, що включається в ціну, визначаємо по наступній формулі:

$$P = (C_{\text{п}} * P) / 100 \quad (2.8)$$

Де  $p$  – плановий рівень рентабельності (10-20%).

$$P = (15076,15 * 10) / 100 = 1507,61 \text{ грн.}$$

## 3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

### Вступ

Безпечні умови праці – не тільки запорука комфортного існування працівників у межах підприємства, а в першу чергу – їх здоров'я та працездатності, а відтак і прибутковості підприємства. Безпека праці на підприємстві може бути на належному рівні тільки тоді, коли всебічно виконуються вимоги трудового законодавства, державних стандартів України, норм і правил, розроблених для збереження здоров'я працюючих.

### 3.1 Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці програмного комплексу

Небезпечним називається фактор, вплив якого на працюючу людину в певних умовах може привести до виробничої травми або іншому раптовому різкому погіршенню здоров'я. Якщо ж виробничий чинник приведе до захворювання або зниження працездатності, то його вважають шкідливим. Залежно від рівня й тривалості впливу, шкідливий чинник може стати небезпечним.

В процесі роботи на користувачів ПК можуть мати вплив наступні небезпечні та шкідливі фактори:

- Невідповідність параметрів мікроклімату нормам;
- Недостатній рівень освітленості;
- Ураження електрострумом;
- Статична електрика;
- Порушення організації робочого місця тощо.

### 3.2 Гігієнічні вимоги до виробничого середовища

У відповідності з Правилами охорони праці під час експлуатації ОТ на робочому місці користувача ПК повинні бути створенні умови для високопродуктивної праці. Розглянемо ці умови.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>55</b>

### 3.2.1 Вимоги до приміщення

Для приміщень, які призначені для роботи з ВДТ, доцільно обрати орієнтацію вікон на північ або на північний схід. На вікнах повинні бути жалюзі, що регулюються, або штори, що дають можливість їх повністю закривати. Приміщення відповідно до ДБН В.2.5-28-2018 «Природне і штучне освітлення» повинні мати природне та штучне освітлення. З приміщеннями ВДТ мають бути обладнані побутові приміщення для відпочинку, психологічного розвантаження тощо.

Площа на одне робоче місце для користувачів повинна складати не менше 6 кв.м, а об'єм – не менше 20,0 куб.м. Стіни пофарбовані матовою фарбою, у відповідності з санітарними вимогами.

### 3.2.2 Освітлення

Для освітлення приміщення, у якому працює користувач ПК, використовується змішане освітлення, тобто сполучення природного й штучного освітлення. Для загального освітлення приміщення використовуються газорозрядні лампи типу ЛД. Норма для необхідної освітленості робочого місця становить 300-500 лк.

### 3.2.3 Шум

При розумовій праці, яка вимагає зосередженості припустимий рівень шуму становить 50дБ. Для зменшення шуму й вібрації в приміщенні устаткування, апарати й прилади встановлюють на спеціальні прокладки, що амортизують. Якщо стіни в приміщенні є джерелами шумоутворення, вони повинні бути облицьовані звуковбирним матеріалом.

### 3.2.4 Мікроклімат

Порушення відповідності ц параметрів мікроклімату впливають на працездатність працівників, їх реакцій, збільшення кількості помилок. Тому в приміщенні повинні бути установлені оптимальні параметри мікроклімату: температура повітря 22-25 °С, вологість повітря – 40-60%, швидкість пуху

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>56</b>

повітря – 0,1-0,2 м/с. Для цього приміщення має бути оснащено системами опалення й кондиціонування, що забезпечують постійне й рівномірне нагрівання, циркуляцію й очищення повітря від пилу й шкідливих речовин.

### **3.2.5 Електробезпека**

Проходячи через організм людини електричний струм робить термічну, електролітичну і біологічну дію.

Для попередження поразок електричним струмом необхідно:

- У повному обсязі виконувати правила провадження робіт і правил технічної експлуатації;
- Виключати можливість доступу працівника до частин устаткування, що працює під небезпечною напругою, неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення;
- Застосовувати ізоляцію, що служить для захисту від поразки електричним струмом.

Для попередження поразок електричним струмом необхідно:

- У повному обсязі виконувати правила провадження робіт і правил технічної експлуатації;
- Виключати можливість доступу працівника до частин устаткування, що працює під небезпечною напругою, неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення;
- Застосовувати ізоляцію, що служить для захисту від поразки електричним струмом.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів ( батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном) мають бути надійно захищені діелектричними щитками або сітками з метою недопущення потрапляння працівника під напругу.

### **3.2.6 Вимоги до організації робочого місця працівника**

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		57

освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео терміналу, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

Робочий стіл повинен регулюватися по висоті в границях 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Рекомендовані розміри столу: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм. Робочий стілець повинен бути оснащений підйомно-поворотним пристроєм для регулювання висоти сидіння і спинки, а також кута її нахилу. Регулювання кожного параметра повинне вироблятися легко, бути незалежним і надійно фіксуватися.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом  $+30^{\circ}$  до нормальної лінії погляду працюючого.

Клавіатуру слід розташовувати на поверхні столу на відстані 100...300 мм від краю, звернутого до працюючого.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам (рис.3.1).

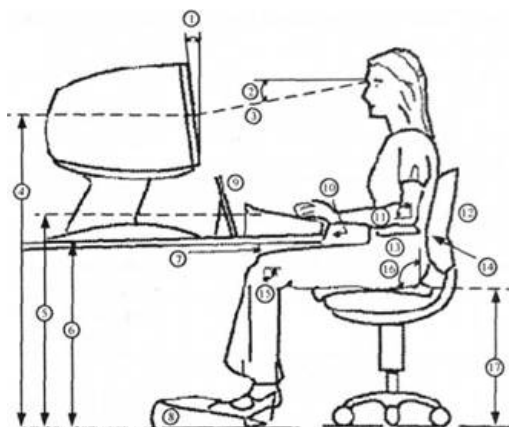


Рисунок 3.1. Робоче місце і робоча поза користувача комп'ютера

1 — кут екрана; 2 — кут огляду (зору); 3 — відстань огляду; 4 — висота середини екрана; 5 — висота клавіатури; 6 — висота столу; 7 — відстань колін від столу; 8 — підставка для ніг; 9 — підставка для документів; 10 — положення рук; 11 — кут ліктів; 12 — спинка крісла; 13 — підлокітник; 14 — опора для попереку; 15 — кут колін; 16 — кут спинки крісла; 17 — висота сидіння

### 3.3 Пожежна безпека

Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки.

Пожежна безпека забезпечується:

- системою запобігання пожежі;
- системою протипожежного захисту;
- організаційно-технічними заходами.

Протипожежний захист приміщення забезпечується застосуванням установки автоматичної пожежної сигналізації, наявністю засобів пожежогасіння, організацією своєчасної евакуації людей.

Для ліквідації невеликих осередків пожеж, а також для гасіння пожеж у початковій стадії їх розвитку силами персоналу об'єктів, застосовуються первинні засоби пожежогасіння. Це вогнегасники (вуглекислотні та порошкові), пожежний інвентар (покривала з негорючого полотна, ящики з піском, бочки з водою), пожежний інвентар.



Рисунок 3.2. Первинні засоби пожежогасіння

## ВИСНОВОК

В дипломній роботі створена система охоронної сигналізації офісу із застосуванням платформи Arduino. Для завдання розробки обрано датчик нахилу, який розміщується на вікна приміщень офісу.

Результати досліджень, виконаних в роботі дозволили встановити, що:

1) застосування симулятора платформи Arduino дає можливість розробляти схема електричну та відповідне програмне за допомогою мови програмування C++ з використанням додаткових бібліотечних функцій пристроїв;

2) застосування мікроконтролера Arduino дозволило підключити 6 датчиків нахилу та 6 світлодіодів для індикації порушень в приміщеннях офісу;

3) у випадку порушення системи охоронної сигналізації запропоновано застосування активного динаміку Piezo, за допомогою якого генерується звуковий сигнал певної частоти для кожного приміщення;

4) у випадку відключення мережі 220 В доцільним є застосування аварійного джерела живлення, до складу якого можна використати акумулятора AGM та перетворювач напруги на 9 вольт.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>60</b>

# ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Технічні засоби охорони периметра: огляд технологій. [Електроний ресурс]. – Режим доступу <http://www.klaster-plus.ua/ua/infocentr/articles/sistemy-okhrany-perimetra/>.

2. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Частина 1: лаб. практик. – Одеса: ОНАЗ ім. О.С. Попова, 2011.

3. Богущ В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.

4. Getting Started with Arduino UNO. [Електроний ресурс]. – Режим доступу: <https://www.arduino.cc/en/Guide/ArduinoUno>.

5. Language Reference. [Електроний ресурс]. – Режим доступу: <https://www.arduino.cc/reference/en>.

6. Arduino Create. [Електроний ресурс]. – Режим доступу: <https://www.arduino.cc/en/main/create>.

7. Beskorovainyi V., Berezovskyi H. Identification of preferences in decision support systems // Econtechmod. An International Quarterly Journal. 2017. Vol. 06, No. 4, P. 15–20.

8. Інтроективний аналіз. Методи та засоби експертного оцінювання / В.В. Крючковський, Е.Г. Петров, Н.А. Соколова, В.Є. Ходеків. Херсон: Гринь ДС, 2018. 284 с. 27. Петров, К. Э., et al. "Компараторна ідентифікація моделі багатофакторного оцінювання альтернатив з використанням методу бегінга." Біоніка інтелекту 2.93 (2019): 21 с.

					<b>КС 57. 19 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		61

# ДОДАТОК А. Слайди мультимедійної презентації

## РОЗРОБКА СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ ОФІСУ

### ДИПЛОМНИЙ ПРОЕКТ

Дипломник: Свирида О.О.  
Керівник: Кільдішев В.Й.

2024

### Основні вимоги до системи охоронної сигналізації офісу



Приклади систем охоронної сигналізації



Приклади систем охоронної сигналізації

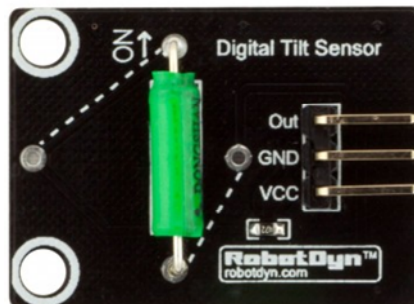


## План офісу для розміщення системи сигналізації

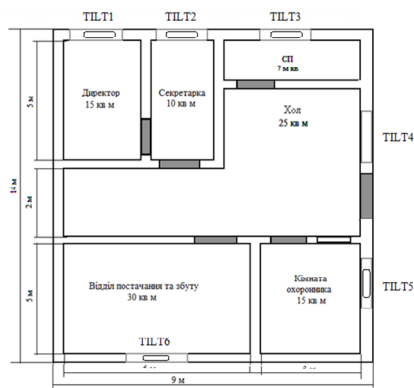


5

## Цифровий модуль Digital Tilt Senso

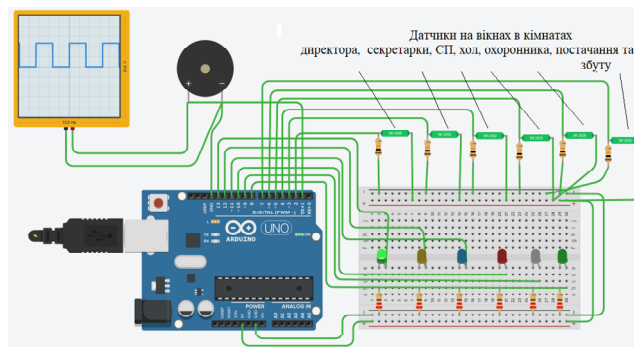


## Розміщення датчиків нахилу в системі Digital Tilt Senso охоронної сигналізації офісу



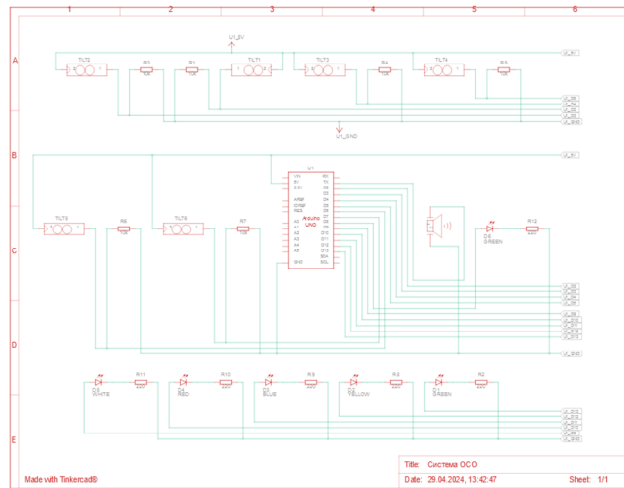
7

## Візуалізація схеми пристроїв системи охоронної сигналізації офісу на основі симулятора



8

## Схема електрична принципіальна системи охоронної сигналізації офісу



### Перелік радіоелементів на схемі

Найменування радіоелемента на схемі	Кількість	Радіоелемент
U1	1	Arduino Uno R3
R1 R3 R4 R5 R6 R7	6	10 kΩ Resistor
TILT1 TILT2 TILT3 TILT4 TILT5 TILT6	6	Tilt Sensor
R2 R8 R9 R10 R11 R12	6	220 Ω Resistor
D1 D6	2	Green LED
D2	1	Yellow LED
D3	1	Blue LED
D4	1	Red LED
D5	1	White LED
PIEZO1	1	Piezo
B	1	Вимикач системи сигналізації

**ДЯКУЮ ЗА УВАГУ!**



# ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

## ВІДГУК

керівника на дипломний проект здобувача освіти  
відділення комп'ютерних систем

Свириди Олександра Олександровича  
(прізвище, ім'я та по батькові здобувача/здобувачки освіти)

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Обслуговування комп'ютерних систем і мереж»

Тема дипломного проекту: «Розробка системи охоронної сигналізації офісу»

### ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над проектом: \_\_\_\_\_

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Проведено огляд сучасних систем охоронної сигналізації. Представлено аналіз вимог до системи охорони периметру об'єкту. Розроблена схема електричної принципальної системи охоронної сигналізації та програмне забезпечення.

в) теоретична підготовка випускника \_\_\_\_\_  
відповідає вимогам, що надаються здобувачу освіти зі спеціальності  
«Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання \_\_\_\_\_

У дипломному проекті розглянуто технології та принципи побудови системи охоронної сигналізації. Наведено оцінка переваг та недоліків існуючих систем. Проектування системи охоронної сигналізації офісу. Проведено аналіз доцільності застосування платформи Arduino для проектування системи сигналізації офісу.

Оцінка розрахункової частини \_\_\_\_\_ 4 (добре)

Оцінка графічної (презентаційної) частини \_\_\_\_\_ 4 (добре)

Загальна оцінка \_\_\_\_\_ 4 (добре)

Прізвище, ім'я, по батькові керівника роботи \_\_\_\_\_ Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи \_\_\_\_\_ к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

« 10 » \_\_\_\_\_ 06 2024 р.

\_\_\_\_\_ В.И.  
(підпис)

\_\_\_\_\_ Кільдішев В.И.

(прізвище та ініціали керівника)

**РЕЦЕНЗІЯ**

на дипломний проект (роботу) студента  
відділення комп'ютерних систем

Свириди Олександра Олександровича

(прізвище, ім'я та по батькові)

Напрямку підготовки 123 «Комп'ютерна інженерія»

Керівник кваліфікаційної роботи

Кільдішев Віталій Йосипович

(прізвище, ім'я та по батькові)

Тема кваліфікаційної роботи

«Розробка системи охоронної сигналізації офісу»

Обсяг пояснювальної записки 67 сторінок

Обсяг графічної (презентаційної) частини проекту 11 аркушів (слайдів)

**ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ**

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідила та проаналізувала методи та засоби захисту сучасних систем охоронної сигналізації.

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Містить базові аспекти щодо використання систем охоронної сигналізації. Запропоновано методи щодо вибору приймально-контрольних приборів в системах охоронно-тривожної сигналізації. Проведено аналіз сучасних систем охоронної сигналізації.

г) перелік позитивних якостей роботи \_\_\_\_\_  
Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.

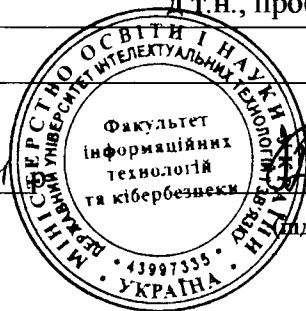
д) основні недоліки роботи У тексті пояснювальної записки присутні помилки оформлення. Для підвищення ефективності захисту було б доцільним провести дослідження сумісного використання систем сигналізації та відеоспостереження.

Оцінка розрахункової частини _____	Добре
Оцінка графічної (презентаційної) частини _____	Добре
Загальна оцінка _____	Добре

Прізвище, ім'я та по батькові рецензента Васіліу Євген Вікторович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку,  
д.т.н., проф. кафедри КБ та ТЗІ

« 14 » 06 2024



(підпис)

Васіліу Є.В.

(прізвище та ініціали рецензента)

Ім'я користувача:  
Катерина Григоріївна Краснокутська

ID перевірки:  
1016324571

Дата перевірки:  
05.06.2024 18:28:02 EEST

Тип перевірки:  
Doc vs Internet + Library

Дата звіту:  
05.06.2024 18:38:52 EEST

ID користувача:  
100011688

Назва документа: 4КС-57\_Олександр\_Свирида

Кількість сторінок: 54 Кількість слів: 8256 Кількість символів: 62006 Розмір файлу: 2.20 MB ID файлу: 1016123302

## 3.43% Схожість

Найбільша схожість: 0.48% з Інтернет-джерелом (<https://suitt.edu.ua/wp-content/uploads/2024/01/ok-19-keruvannia-do>).

3.43% Джерела з Інтернету

480

Сторінка 56

Не знайдено джерел з Бібліотеки

## 0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

1

**ДОЗВІЛ  
НА РОЗМІЩЕННЯ  
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ  
(ДИПЛОМНОГО ПРОЕКТУ)  
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»**

Ми, що нижче підписалися,

**Свирида Олександр Олександрович,**  
здобувач освіти гр. 4КС-57, та

**Кільдішев Віталій Йосипович,**  
керівник дипломного проекту,

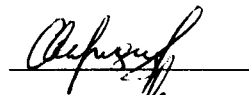
не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

**«Розробка системи охоронної сигналізації офісу» (автор роботи – Свирида О.О., керівник роботи – Кільдішев В.Й.)**

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2024 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

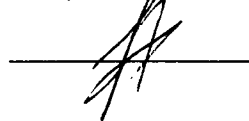
Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець



/ Свирида О.О. /

Керівник



/ Кільдішев В.Й. /

«10» червня 2024 р.