

Вінницький національний технічний університет  
Факультет інформаційних технологій та комп'ютерної інженерії  
Кафедра захисту інформації

## **Пояснювальна записка**

до магістерської кваліфікаційної роботи  
на тему: «Інтелектуальна система охоронно-тривожної сигналізації  
промислового об'єкту»  
08-20.МКР.004.00.000 ПЗ

Виконав: студент 2 курсу, групи 1БС-18(м)  
Спеціальність – 125 Кібербезпека

\_\_\_\_\_ Губчакевич С.А.

Керівник: к. т. н., доц. каф. ЗІ

\_\_\_\_\_ Куперштейн Л. М.

Рецензент: к.т.н. проф. каф. ОТ

\_\_\_\_\_ Азарова А. О.

Вінниця – 2019 р.

Вінницький національний технічний університет  
Факультет Інформаційних технологій та комп'ютерної інженерії  
Кафедра Захисту інформації  
Освітньо-кваліфікаційний рівень магістр  
Спеціальність – 125 Кібербезпека

**ЗАТВЕРДЖУЮ**  
д.т.н., проф. зав. кафедри ЗІ  
\_\_\_\_\_ В. А. Лужецький  
“ \_\_\_\_\_ ”  
\_\_\_\_\_ 2019 року

## **З А В Д А Н Н Я** **НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Губчакевичу Сергію Анатолійовичу

1. Тема роботи: «Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту»  
керівник роботи: Куперштейн Леонід Михайлович, к.т.н., доц. кафедри ЗІ, затверджені наказом ректора ВНТУ від \_\_\_\_\_ 2019 року № \_\_\_\_\_
2. Строк подання студентом роботи \_\_ грудня 2019 р.
3. Вихідні дані до роботи:
  - мова програмування – C/C++;
  - модульність системи;
  - можливість роботи з GSM пристроями;
  - платформа для розробки – Arduino;
  - наявність автономного живлення;
  - наявність додатку для керування системою;
  - інтелектуальні правила для користування системою
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ. 1. Аналіз існуючих охоронно-тривожних систем захисту підприємства. 2. Реалізація апаратної частини. 3. Реалізація програмної частини та тестування 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу  
Типова структура охоронно-тривожних систем (плакат, А4). Схема розміщення давачів в складському приміщенні підприємства (плакат, А4). Загальний

алгоритм роботи системи (плакат, А4). Алгоритм відключення давачі охоронно-тривожної сигналізації (плакат, А4). Загальна структура системи (плакат, А4). Макет додатку для керування системою (плакат, А4).

#### 6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<b>1</b>	Куперштейн Л.М., к.т.н., доц. каф.ЗІ		
<b>2</b>	Куперштейн Л.М., к.т.н., доц. каф.ЗІ		
<b>3</b>	Куперштейн Л.М., к.т.н., доц. каф.ЗІ		
<b>4</b>	Мацкевичус С.С., ст. викл. каф. ЕПВМ		

7. Дата видачі завдання \_\_\_\_\_ року.

### КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2019 – 04.09.2019	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	05.09.2019 – 15.09.2019	
3	Науково-технічне обґрунтування	16.09.2019 – 22.09.2019	
4	Розробка технічного завдання	23.09.2019 – 29.09.2019	
5	Розробка рішень	30.09.2019 – 12.10.2019	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2019 – 10.11.2019	
7	Розробка розділу економічного обґрунтування доцільності розробки	11.11.2019 – 17.11.2019	
8	Аналіз виконання ТЗ, висновки	18.11.2019 – 24.11.2019	
9	Оформлення пояснювальної записки	25.11.2019 – 30.11.2019	
10	Попередній захист та доопрацювання МКР	28.11.2019 – 01.12.2019	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2019 – 10.12.2019	
12	Представлення МКР до захисту	11.12.2019 – 14.12.2019	
13	Захист МКР	16.12.2019 – 20.12.2019	

Студент \_\_\_\_\_ Губчакевич С.А.  
( підпис )

Керівник роботи \_\_\_\_\_ Куперштейн Л.М.  
( підпис )

## **АНОТАЦІЯ**

Магістерська кваліфікаційна робота присвячена розробці інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту. В ході роботи було проведено наукове дослідження з обґрунтуванням доцільності розробки. Проведено аналіз типової структури охоронно-тривожних систем. Визначено основний перелік датчиків, котрі контролюють периметр приміщення, та наведено основні інтелектуальні правила системи, які відрізняють її від аналогів. Розроблено мобільний додаток для керування системою. В економічному розділі оцінено затрати на розробку та її доцільність.

## **ABSTRACT**

The master's qualification is dedicated to the development of an intelligent alarm and alarm system for an industrial site. During the work, a scientific study was conducted to substantiate the feasibility of development. The typical structure of security and alarm systems is analyzed. The basic list of sensors that control the perimeter of the room is determined, and the basic intellectual rules of the system that distinguish it from analogues are given. A mobile application for system management has been developed. The economic section estimates development costs and their feasibility.

## ЗМІСТ

ВСТУП.....	5
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ.....	7
1.1 Науково технічне обґрунтування теми МКР.....	7
1.2 Аналіз структури типових охоронно-тривожних систем.....	9
1.3 Аналіз існуючих систем охоронно-тривожної сигналізації.....	13
1.4 Формалізація вимог та постановка задачі.....	19
2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ОХОРОННО-ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ.....	21
2.1 Аналіз структури підприємства та схема розміщення компонентів пристрою.....	21
2.2 Розробка загальної структури апаратного засобу.....	23
2.3 Інтелектуальний режим системи охоронно-тривожної сигналізації.....	28
2.4 Обґрунтування вибору компонентів системи.....	30
3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ.....	39
3.1 Розробка програмної частини системи.....	39
3.2 Розробка програмної частини додатку для керування системою.....	41
3.2 Тестування пристрою.....	43
4 ЕКОНОМІЧНА ЧАСТИНА.....	47
4.1 Технологічний аудит розробленої інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту.....	47
4.2 Розрахунок витрат на розробку інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту.....	53
4.3 Розрахунок економічного ефекту від можливої комерціалізації нашої розробки.....	56
ВИСНОВКИ.....	61
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	62
ДОДАТОК А.....	64
ДОДАТОК Б.....	70
ДОДАТОК В.....	79

## ВСТУП

У зв'язку з край нестабільним політичним і економічним кліматом в країні, а також з постійно зростаючою кількістю техногенних катастроф, кримінальних дій, на першому місці виходять завдання з вирішення питань особистої безпеки громадян так і питання безпеки житла, бізнесу.

Загальна стратегія захисту полягає в виявленні несанкціонованого доступу до приміщення чи небезпечного події; локалізації місця і джерела події; здійсненні дій, що перешкоджають розвитку події; документуванні часу, місця і змісту події; заходів щодо усунення негативних наслідків події. У минулому стратегія захисту об'єкта базувалася на організації спеціалізованих служб охорони із залученням великої кількості навчених людей, які несли цілодобове чергування, обходили всі потенційно небезпечні ділянки об'єкта, контролювали справність роботи всіх систем і перешкоджали проникненню сторонніх осіб на об'єкт.

Забезпечення ефективної системи безпеки об'єктів і територій потребує вирішення цілого комплексу завдань [1], пов'язаних як із участю людини, так і з наявністю різних систем безпеки: сигналізації, відеоспостереження, тощо. Своєчасно отримана інформація дозволяє зводити наслідки будь-яких надзвичайних подій до мінімуму, а головне зберігати життя людей та їхнє майно. Ця задача вирішується за допомогою забезпечення безпеки: комплексу дистанційної сигналізації. На сьогоднішній день технології дозволяють створювати системи, які своєчасно попереджають про настання або наближення тих чи інших подій. Різноманітність ситуацій у нашому житті піднімає проблему своєчасного сповіщення на інший рівень. Наприклад, при нападі злочинців на власний дім, людина може бути проінформована миттєво, щоб уникнути несприятливих наслідків і дати більше часу щоб прийняти заходи для вирішення проблеми. Останнім часом на ринку надання послуг систем безпеки запропоновано велику кількість рішень, що істотно відрізняються як апаратним та програмним забезпеченням, так і пов'язаними з цим функціональними можливостями комплексів, а, відповідно, і вартістю [2]. В даному проекті реалізовано максимально бюджетну, порівняно з тим що представлено на ринку, систему. Особливістю цього пристрою є розширений набір датчиків, котрі охоплюють весь контроль за об'єктом і набір інтелектуальних правил, котрі завдяки своїй продуманості будуть максимально ефективними для будь-якого об'єкта захисту.

**Об'єкт дослідження.** Об'єктом дослідження є системи охоронно-тривожних сигналізацій для забезпечення безпеки територій або приміщень.

**Предмет дослідження.** Предметом дослідження є методи захисту промислових приміщень від несанкціонованого доступу.

**Мета роботи.** Метою магістерської кваліфікаційної роботи є підвищення захищеності підприємства від зовнішнього фізичного проникнення на територію за рахунок розробки та впровадження апаратного засобу на територію підприємства. Розроблювальний пристрій пристосується до будь-якого підприємства, яке має складське приміщення.

Для досягнення мети необхідно розв'язати такі задачі:

- виконати науково-технічне обґрунтування розробки;
- дослідити та проаналізувати існуючі методи та засоби захисту програмно-технічного захисту;
- допрацювати існуючий апаратний засіб, шляхом додавання важливих давачів та впровадженням логічних і інтелектуальних правил;
- виконати тестування розробленого апаратно-програмного засобу;
- визначити економічний ефект від розробки системи охоронно-тривожної сигналізації.
- розробити рекомендації щодо впровадження та експлуатації засобу захисту.

**Наукова новизна.** Запропоновано інтелектуальну модель режиму роботи системи охоронно-тривожної сигналізації, який полягає у використанні вагових коефіцієнтів для кожного із давачів для формування сповіщення.

**Практична цінність.** Практична цінність роботи полягає у тому, що розроблено автономну інтелектуальну систему охоронно-тривожної сигналізації для промислового об'єкту у вигляді програмно-апаратного комплексу на базі мікроконтролерної платформи Arduino та мобільного додатку для ОС Android, що передбачає швидке управління системою і перегляді системної інформації.

В сукупності з обширною кількістю давачів систему можна ефективно використовувати для захисту комерційного продукту. Окремі результати роботи доповідались на XLVII та XLVIII Науково-технічних конференціях підрозділів Вінницького національного технічного університету в 2018р. та 2019р.

## 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

### 1.1 Науково технічне обґрунтування теми МКР

Останнім часом в Україні, стала найбільш актуальна проблема безпеки об'єкта, а також проблема інформаційної безпеки [2]. Динаміка росту несанкціонованого доступу до приміщень є досить важливою проблемою для Вінницької області. На рисунку 1.1 зображена динаміка росту несанкціонованих проникнень до приміщень.

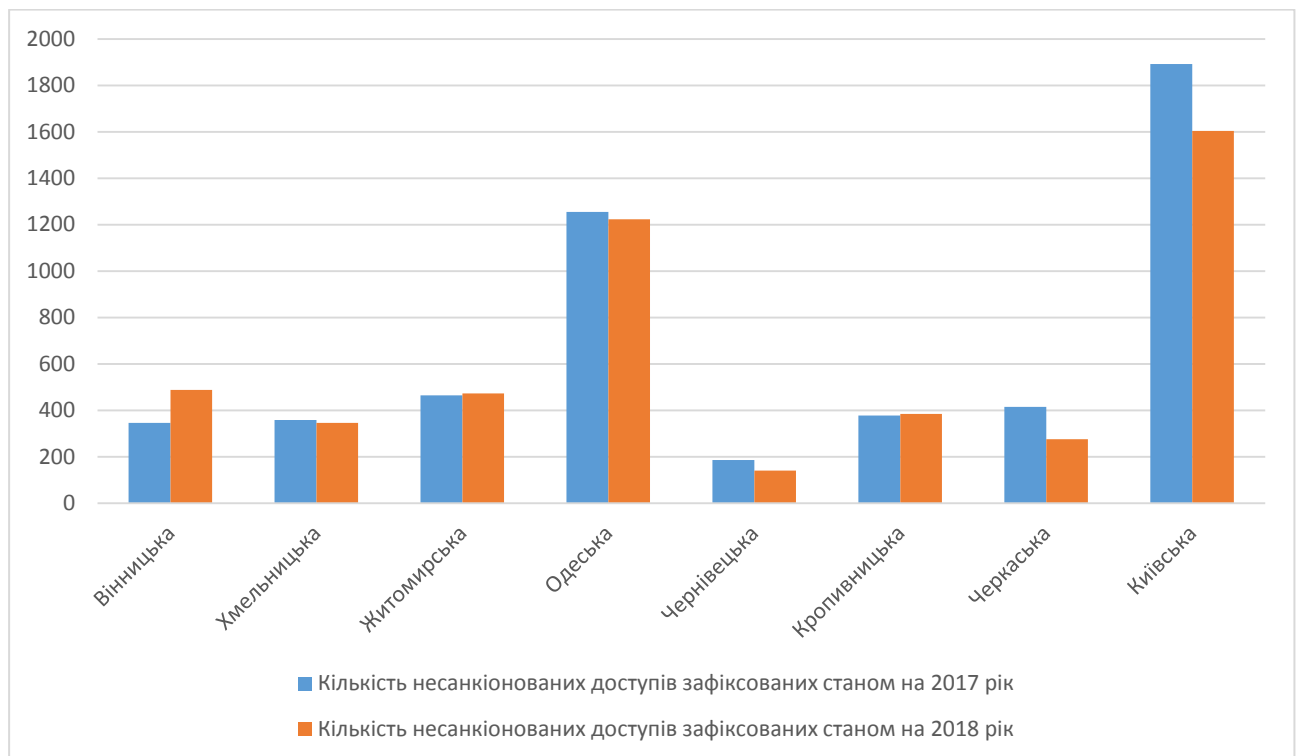


Рисунок 1.1 – Динаміка проникнень на підприємства по сусіднім областям Вінницької області

Як можна побачити з графіків, динаміка росту для Вінницької області є найбільшою з усіх сусідніх, тобто можна побачити, що ця залежність зростає, і таким чином виникає необхідність захисту приміщень/підприємств від несанкціонованого доступу за рахунок охоронно-тривожних систем, оскільки наразі інші методи захисту не є ефективними [3]. Системи охоронно-тривожних сигналізацій є одною з головних перешкод на шляху до несанкціонованого проникнення на об'єкт. В зв'язку з широким використанням сучасних охоронно-тривожних систем відбувається істотна "інтелектуалізація" технічних засобів охорони. Сучасні системи захисту перестають бути просто допоміжними і набувають нових властивостей [4], що робить істотний вплив на організацію



охорони і її рівень. Сучасні технічні засоби охорони можуть бути використані у вигляді повністю інтегрованої системи або системи, що складається з функціонально незалежних компонентів:

- охоронно-тривожна сигналізація,
- система контролю доступу в приміщення з перевіркою повноважень,
- система телевізійного спостереження
- контрольні та інші пристрої.

Охоронна сигналізація використовується вже дуже давно, і давно перестала бути чимось екзотичним. Практично кожен другий магазин, офіс, склад мають охоронну сигналізацію. Принцип дії охоронної сигналізації дуже простий. Інсталюються системи розглядаються і вивчаються місця можливого проникнення на об'єкт, в свою чергу на ці критично важливі контрольні точки встановлюються датчики, які блокують можливе несанкціоноване проникнення (в цьому плані найбільш уразливими з точки зору безпеки є вікна, двері, шахти провітрювання). У приміщенні охорони встановлюється прилад охоронної сигналізації. В разі відкриття дверей, вікна, розбитті скла, і при загальному несанкціонованому проникненні в офіс/установу, спрацьовує відповідний датчик, і сигнал передається на прилад охоронної сигналізації в приміщенні охорони [5].

Такий алгоритм в загальному актуальний для великих підприємств, котрі не шкодують вкладати кошти в власну безпеку. Щодо підприємств меншого масштабу все складніше. Сучасний стан речей не дозволяє використовувати якісну охорону, оскільки це коштує чималих витрат, а якщо розглядати власноручне встановлення і використання систем охоронно-тривожної сигналізації, то виникають складнощі з підбором устаткування і його експлуатацією, бо функціонал не завжди оправдовує себе в тій чи іншій ситуації, а якісні системи в основному заточені під певні об'єкти, де набори датчиків підбираються виключно з замовником системи і враховуючи всі особливості приміщення, а системи з більш демократичним цінником часто мають неякісну апаратну/програмну частини та обмежений набір датчиків, хоча в свою чергу вони є більш універсальними для установки в будь-яке приміщення. Тому вибір падає на GSM системи, оскільки вони є більш доступними в ціновому діапазоні, і їхнє встановлення і обслуговування не є складним процесом.

Розглянемо загальну схему роботи основних GSM охоронно-тривожних систем [5] які представлені на ринку на сьогоднішній момент, яка зображена на рисунку 1.2.



Рисунок 1.2 – Схема роботи GSM – сигналізації

Основними недоліками кожного з представників свого цінового сегменту, про який ми поговоримо пізніше, на ринку сучасних охоронно-тривожних систем є як обмежений функціонал (а саме можливість задання лише одного номера для керування чи обмежений набір давачів), цей недолік частково усувається в системах більш дорожчих, проте проблема завжди залишається в тому, що немає балансу між функціоналом та ціною. Варто додати, що апаратна складова таких систем часто перевищує собівартість майже в десятки разів. Дешевші представники пропонують опосередкований набір давачів (в основному датчики руху і магнітогерконові давачі), а з функціоналу лише сповіщення і переведення в режим роботи.

Отже, встановивши основну проблему, яка присутня для даної сфери на сьогоднішній момент, а саме:

- обмежений функціонал;
- обмежена апаратна складова;
- неякісний набір апаратної складової;
- досить велике завищення цін на усі пристрої.

Визначивши, основні проблеми можна перейти до її вивчення більш детально, а саме розгляду існуючих аналогічних систем, які наразі представленні на ринку і порівняння їх з розробленим пристроєм.

## 1.2 Аналіз структури типових охоронно-тривожних систем

Принцип роботи GSM-сигналізації заснований на використанні технології стільникових мереж. Тривожний сигнал миттєво передається з об'єкта на центральний пульти, в якості якого виступає смартфон власника системи.

Функціональні завдання у такого комплексу такі же, як і інших охоронних систем. Він оперативно виявляє потенційну загрозу і реагує відповідно до встановленого алгоритму. Із цією метою використовуються різні типи датчиків (відкриття дверей, вікон, руху), прилад обробки і передачі даних.

Паралельно з відправкою сигналу, у деяких представників відбувається управління виконавчими пристроями, світловими приладами, сиренами.

У стандартний набір обладнання охоронного комплексу [6], в загальному випадку, входять:

- 1) Охоронний прилад.
- 2) Датчик руху.
- 3) Датчик відкриття дверей / вікна.

Розширити його можна додатковим обладнанням, яке обговорюється з майбутнім замовником окремо, для покриття усіх можливих точок для несанкціонованого доступу.

Принцип роботи охоронної сигналізації має на увазі використання вбудованого GSM-модуля. З його допомогою сигнал передається на центральний охоронний пульт, який в свій час оброблює дані та відправляє їх власникові системи. За способом повідомлення охоронну сигналізацію, поділяють на такі види:

Автономні системи – системи які передбачають оснащення об'єктів датчиками, які при проникненні спрацьовують, включаючи звукову сирену, або пристрої зі спеціальними світловими спалахами [6]. Всі пристрої підключені до загальної контрольної панелі, на яку передається сигнал від того чи іншого датчика. На пульт зовнішньої охорони сигнал про порушення не передається.

Системи охоронної сигналізації з підключенням за допомогою телефонної лінії - принцип роботи такої системи досить простий та популярний [6]. При спрацьовуванні системи включається спеціальний модуль, що відправляє голосові повідомлення на заздалегідь запрограмовані номери абонентів, таким чином, подається сигнал про проникнення порушника. Абонентами, як правило виступають охоронні служби. GSM-системи – в цьому випадку сигнали від датчиків сигналізації передаються на спеціальний GSM-модуль. При спрацьовуванні сигналізації система передає тривожні повідомлення у вигляді SMS, або ж голосові сигнали на запрограмовані мобільні телефони відповідальних осіб. Централізована система з виходом на пульт сигналізації – на сьогоднішній день найбільш ефективна система охоронної сигналізації. При спрацьовуванні охоронних датчиків, сигнал з панелі сигналізації направляється на пульт охорони. Для зв'язку з центральним пультом можуть використовуватися та GSM-лінії, та телефонні канали, та

радіоканали, а також спільне, або комбіноване поєднання перерахованих вище ліній.

Всім перерахованим вище охоронним системам, за винятком GSM-сигналізації, притаманний ряд недоліків:

1) при активації тільки сирени або світлової сигналізації немає можливості оповіщення користувача про тривогу, якщо його немає в безпосередній близькості до охоронного об'єкту, щоб почути сирену або світлову сигналізацію. Дана система виконує лише функцію привертання уваги.

2) система сигналізації з підключенням до телефонної лінії. Телефонну лінію можна обрізати. Можливі також і інші пошкодження телефонної лінії - дана система не автономна.

3) пультова охорона, як і попередня, з'єднується з пультом охорони за допомогою дротів, при пошкодженні проводів система перестає працювати.

Виходячи з цього, розробка засобів контролю за віддаленими об'єктами на основі технології GSM охорони є перспективною і актуальним завданням.

Принцип роботи більшості охоронно-тривожних систем схожий [7]. На рисунку 1.3 зображено типову структуру таких систем.

Після включення живлення або натискання кнопки ON пристрій входить в той режим, в якому було останній раз - "очікування постановки на охорону" або "охорона".

У режимі "очікування постановки на охорону" пристрій чекає на команду чи ключ на ввімкнення режиму "охорона". Якщо ж хоч одна з зон не закрита, то пристрій моргне три рази короткими спалахами і не встане в режим "охорона". Закритою зоною вважається зона, яка закорочена на землю. Якщо не потрібно всі чотири зони, то зайві повинні бути теж закриті. Якщо ж команди або ключа немає в пам'яті, то світлодіод також моргне три рази.

У режимі "охорона" світлодіод зрідка моргає, опитуються всі зони на розрив і перевіряється наявність зовнішнього живлення. При розриві будь-який з зон на номери телефонів, занесені в пам'ять GSM-модуля, відправляються СМС і надходять короточасні виклики. Після чого світлодіод починає швидко моргати, і пристрій очікує виходу з цього режиму за допомогою команди. Якщо в цьому режимі відбудеться відключення зовнішнього живлення, то на всі номери одноразово прийде SMS з відповідним текстом, а пристрій, як уже було сказано, буде продовжувати роботу від акумулятора.

Блок давачів відповідає за виявлення і ідентифікацію загроз. В нього входять в основному давач руху та давач відкриття дверей. Блок обробки даних включає в себе мікроконтролер, який обробляє інформацію з давачів, після чого

направляє її на блок передачі даних, який часто включає в себе GSM-модуль, який направляє сигнал тривоги отримувачеві.

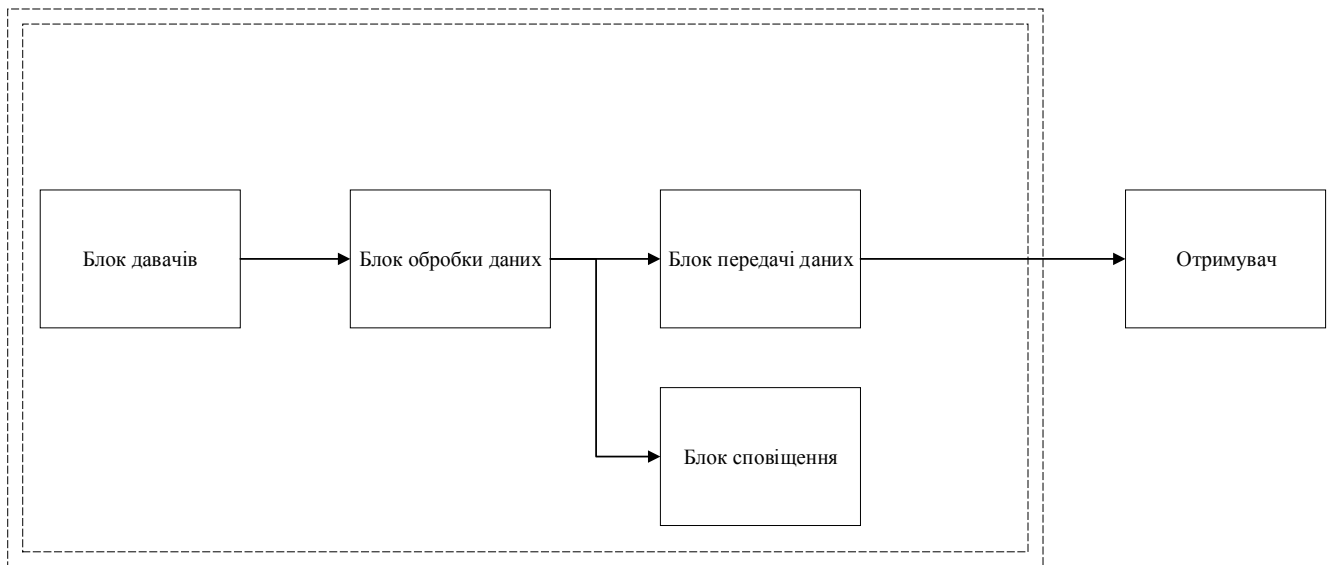


Рисунок 1.3 - Типова структура охоронно-тривожних систем

Розглянемо основу архітектури типових охоронно-тривожних систем і розділимо їх на логічні рівні.

Перший рівень – давачі [7]. Давачі часто інтегруються як компонент системи, який автоматично виконує задачу або попереджає користувача про спрацювання в певній області. Вони формують життєво важливий компонент безпеки в охоронно-тривожних системах, автоматизованих системах, системах управління розумним будинком.

Другий рівень – мікроконтролер [7]. Мікроконтролер є основними мізками системи на єдиній інтегральній схемі. В сучасній термінології - це система на мікросхемі або SoC. Мікроконтролер містить один або кілька центральних процесорів (ядра процесора) разом з пам'яттю і програмованими периферійними пристроями введення / виводу.

Третій рівень - мережа передачі даних [7]. Мережа передачі даних - мережа зв'язку, яка дозволяє вузлам спільно використовувати ресурси. У мережах передачі даних мережеві обчислювальні пристрою обмінюються даними один з одним використовуючи канал передачі даних. З'єднання між вузлами можуть бути встановлені за допомогою кабельних або бездротових носіїв.

Четвертий рівень – рівень обробки [7]. Такий рівень присутній у системах з великим ціновим діапазоном. Основна його суть – виведення інформації про давачі і керування ними через додаток, пуль керування або веб-інтерфейс.

Реалізація останнього рівня не завжди доцільна, оскільки слід комплексно враховувати структуру підприємства і доцільність такого рівня під конкретний об'єкт захисту надійних систем захисту програмного забезпечення від комп'ютерних злочинів.

### **1.3 Аналіз існуючих систем охоронно-тривожної сигналізації**

Будь яке підприємство чи установа потребує захисту від проникнення зловмисників, саме тому попит на сигналізації тільки постійно зростає. Розглянемо системи які вже присутні на ринку.

Основою для більшості GSM-сигналізацій є саме мікроконтролер [8]. Мікроконтролер - це спеціальна мікросхема, призначена для керування різними електронними пристроями. Мікроконтролери вперше з'явилися 1971 р.

Розробники мікроконтролерів придумали дотепну ідею – об'єднати процесор, пам'ять, ПЗП і периферію всередині одного корпусу, зовні схожого на звичайну мікросхему. З тих пір виробництво мікроконтролерів щорічно у багато разів перевищує виробництво процесорів, а потреба в них не знижується.

Мікроконтролери випускають десятки компаній, причому виробляються не тільки сучасні 32-розрядні мікроконтролери, але і 16, і навіть 8-бітні (як i8051 і аналоги). Всередині кожного сімейства часто можна зустріти майже однакові моделі, що розрізняються швидкістю роботи ЦПУ і об'ємом пам'яті.

Справа в тому, що мікроконтролери застосовуються переважно у вбудованих системах, в іграшках, у верстатах, у масовій домашньої техніки, домашньої автоматики – там, де не потрібна потужність процесора, а, швидше, баланс між ціною і достатньою функціональністю .

Саме тому найбільш старі типи мікроконтролерів ще досі в ходу – вони багато чого можуть: від автоматичного відкривання дверей і включення поливу газонів до інтеграції в систему «розумний будинок» . При цьому існують і більш потужні мікроконтролери, здатні виконувати сотні мільйонів операцій в секунду і обв'язані периферією «до зубів». У них і відповідні завдання. Таким чином, розробник спочатку оцінює завдання, а вже потім вибирає під неї відповідне «залізо».

Майже всі GSM – сигналізації на ринку мають більш-менш схожий набір модулів. В основному це давач руху. Слід порівняти між собою

мікроконтролери, які на ринку користуються найбільшою популярністю, порівняльні характеристики [8] зображені в таблиці 1.1.

Таблиця 1.1 – Порівняльна характеристика популярних мікроконтролерів

Характеристики	STM32	ATmega328	PIC16F84A	ATTINY2313
Частота, МГц	72	16	20	20
Пам'ять, кБайт	64	32	32	1
Живлення, В	3.3	5	5	5
ОЗП, кБайт	20	2	2	0.128
USB 2.0	+	-	-	-
DMA	+	-	-	-
CAN	+	-	-	-
RTC	+	-	-	-
UART	3	1	1	1
Прошиття через USB	-	+	+	-
Ціна	2.1\$	1.8\$	2.9\$	1.7\$

Виходячи з даної таблиці, можна побачити що мікроконтролер STM лідирує майже по всім параметрам, проте для вирішення задач дипломної роботи достатньо і мікроконтролера ATmega. Мікроконтролер Arduino має попри все великий плюс, а саме велика і обширна база знань і відповідей в СНД, яка включає в себе тисячі бібліотек та готових модульних рішень, а оскільки метою дипломної роботи є створити комплексну систему охоронно-тривожної сигналізації за мінімальною ціною та з притаманними системі інтелектуальними правилами, було обрано мікроконтролер Arduino.

Асортимент ринку охоронно-тривожних сигналізацій величезний. Розглянемо їх склад, основні відмінні риси, принцип роботи, наскільки виправдано їх застосування, які витрати на експлуатацію та сервісне обслуговування.

Основна складова всіх охоронних сигналізацій - сповіщувачі (датчики), які визначають контрольовану подія і відправляють сигнал на контрольну панель. Давачі розпізнають практично всі фізичні явища, такі як рух об'єктів, зміна температури в приміщенні, задимленість, загазованість, заливка водою, вібрації і шум (при розбитті скла), відключення електрики, і інші зміни і явища, створювані при певних діях порушника або комунікацій.

Охоронні сигналізації поділяються в основному за [9]:

1) за способом зв'язку кінцевих датчиків з контрольною панеллю на:

- провідні – датчики яких з'єднуються по проводам з самою системою;
- бездротові – датчики яких з'єднуються з системою по бездротових мережах.

2) за способом оповіщення (інформують господаря або службу реагування) про виявлений подію на:

- оповіщення по радіоканалу. Дальність дії до 5 км. Дані сигналізації застосовуються в разі постановки на охорону і моніторинг найближчого КПП або службі реагування. У такому випадку інформація безпосередньо господареві не надходить.

- оповіщення по GSM каналу (через SMS-повідомлення). Дальність дії необмежена і визначається доступністю абонентів, яким відправляється SMS-повідомлення з інформацією про спрацьовування будь-якого датчика.

- оповіщення по лінії телефону. Контрольна панель повинна бути підключена до телефонної лінії, тому застосовується в квартирах, де є стаціонарний телефон.

- оповіщення по супутниковому каналу. Дальність дії необмежена.

У провідних системах сигнал від датчиків надходить до контрольної панелі по кабелям, спеціально прокладеним від кожного датчика до контрольної панелі. Таким чином, у Бездротових систем є перевага по монтажу, оскільки їх можна монтувати після ремонту, не проводячи конструктивних робіт з прокладання проводів.

Розглянемо більш детально бездротові охоронні сигналізації. Кожен елемент бездротової охоронної сигналізації, будь то інфрачервоний датчик руху або магнітогеркований датчик, датчик диму або датчик протікання води, оснащений радіопередавачем для відправки сигналу на контрольну панель. Деякі елементи, наприклад сирена, мають ще радіоприймач для отримання керуючого сигналу на контрольну панель.

Сигнали посилаються в зашифрованому вигляді і поділяються на:

- Контрольні - про спрацьовування на зовнішній вплив.
- Службові (тестові) - про індикації рівня сигналу.

Поява на українському ринку бездротових охоронно-тривожних сигналізацій було обумовлено дозволами на використання спеціальних частот і також появою зарубіжних систем, які позитивно зарекомендували себе серед кінцевим користувачам - власників приватної нерухомості. Ціна проводового датчика, як правило, нижче ціни аналогічного бездротового. Крім того, основною перевагою бездротових датчиків є менший ступінь зношеності елементів живлення системи.



Основною причиною популярності бездротових охоронно-тривожних систем є такі причини:

1) У приватних об'єктах установка потрібно, як правило, після проведених оздоблювальних робіт. Прокладка кабелю від датчика до контрольної панелі (зовнішня або прихована) може об'єктивно потребувати великих витрат на монтаж дротяних датчиків, особливо у великому приміщенні.

2) Час установки бездротових датчиків і, відповідно, здачі охоронної сигналізації в експлуатацію істотно менше. Мінімальний комплект фахівець може налаштувати і встановити за 2-3 години.

3) Нарощування функціональності сигналізації завдяки додаванню нових датчиків може бути здійснено в будь-який час і досить оперативно - в контрольній панелі реєструється новий датчик, прописується необхідна реакція сигналізації (наприклад, новий текст SMS-повідомлення або включення сирени), датчик прикручується в необхідному місці.

Таким чином, у кінцевого користувача тепер є вибір: заощадити на монтажі та прокладанні кабелів або на кінцевому обладнанні.

Розглянемо три аналога найбільш популярних на сьогоднішній момент на ринку. Мета порівняння полягає в підтвердженні факту актуальності і необхідності кінцевого електронного засобу в споживчому сегменті ринку [9].

Система "Страж SMS 8x6 GPS", вигляд якої зображено на рисунку 1.4, призначається для контролю приміщень і автомобілів, а так само для управління віддаленими об'єктами [9].



Рисунок 1.4 – Вигляд типового представника ринку «Страж SMS 8x6 GPS»

Основними недоліками даної системи охоронно-тривожної сигналізації є такі пункти:

- 1) Кількість датчиків стандартної комплектації – 2 шт.
- 2) Відсутність автономного живлення.
- 3) Мала кількість номерів для сповіщення – 1 шт.

4) Відсутність інтелектуальної частини в функціоналі пристрою.

Система "Visonic GA-1RS", яка зображена на рисунку 1.5, призначається для контролю приміщень на прикладі невеликих офісних будівель [9].



Рисунок 1.5 – Вигляд типового представника ринку «Visonic GA-1RS»

Основними недоліками даної системи охоронно-тривожної сигналізації є такі пункти:

- 1) Кількість давачів стандартної комплектації.
- 2) Мала кількість номерів для сповіщення – 1 шт.
- 3) Відсутність інтелектуальної частини в функціоналі пристрою.
- 4) Відсутність світлового сповіщення на об'єкті захисту.
- 5) Відсутність контрольного дзвінка адміністратору системи.

«Страж-GSM-M», вигляд системи зображено на рисунку 1.6, призначений для охорони квартир, офісів, дач, автомобілів та інших об'єктів охорони та здійснює оповіщення через мережу стільникового зв'язку стандарту GSM за допомогою дзвінка на задані телефонні номери (до 3-х номерів) [9].



Рисунок 1.6 – Вигляд типового представника ринку «Страж-GSM-M»

Основними недоліками даної системи охоронно-тривожної сигналізації є такі пункти:

- 1) Кількість давачів обмежена - 1 шт.

- 2) Відсутність автономного живлення.
- 3) Відсутність сирени чи світлового сповіщення.
- 4) Відсутність інтелектуальної частини в функціоналі пристрою.

Звернемо увагу на велике число подібностей і не принципове технічне відмінність розглянутих пристроїв. Не дивлячись на це, ціновий діапазон даних представників є досить важким для середнього класу громадян.

Недоліками кожного з представників є як обмежений функціонал вітчизняних виробників так і завищена ціна, також варто відмітити відсутність автономного живлення в деяких екземплярах, адже це є важливою складовою в захисті об'єкту і захищає приміщення в будь-який момент часу [10]. Недоліком китайського виробника є вразливість до перехвату сигналу з давача, оскільки вони використовують безпроводні давачі і також, відсутній певний функціонал в порівнянні з розробляючим пристроєм.

Основною перевагою розроблюваного пристрою є присутність інтелектуальних правил та груп, які будуть задаватись програмним шляхом, наявність автономного, об'ємного живлення та її простота в використанні за допомогою додатку під ОС Android. Основні контрольні переваги над існуючими аналогами, окрім дешевизни такої системи, відображені нижче, а також в таблиці 1.2:

- 1) Перевірка доступності кожного з давачів в заданий проміжок часу (10-12 секунд) і при їх недоступності – сповіщення власника системи.
- 2) Контрольний дзвінок користувачам адміністративної групи.
- 3) Автономна робота від акумулятору до 16 годин (у існуючих аналогів акумуляторна батарея або відсутня, або має досить малу ємність, що полегшить зловмисникам несанкціонований доступ.
- 4) Комплексний захист площі за рахунок великої кількості давачів, які покривають всі територіальні аспекти підприємства
- 5) Можливість додавання користувача системи до груп адміністрування (до прикладу лише певна група користувачів зможе ставити систему в робочий режим чи керувати певним давачем).
- 6) Незалежність від WiFi, Ethernet (користувачу в будь-який момент часу і на будь-якій відстані від системи отримає сповіщення про той чи інший інцидент), та можливість відключення окремого давача від системи.

Таблиця – 1.2 Характеристики прототипів

Характеристика	SMS 8x6 GPS	GA-1RS	GSM-M	LL2000
Кількість давачів	2	1	1	2
Ціна грн	3200	3750	2500	3680

Продовження таблиці 1.2

Наявність GSM	+	+	+	+
Складність користування	-	+	-	-
Автономне живлення	-	400мА	-	450мА
Давач руху	+	+	+	+
Сирена	+	+	-	+
Світлове сповіщення	-	-	-	-
Давач відкриття дверей	+	-	-	+
Давач шуму	-	-	-	-
Давач вібрацій	-	-	-	-
Давач тиску	-	-	-	-
Пульт керування	-	+	-	+
Сповіщення по відключенню давача	-	-	-	-
Адміністративна група	+	-	-	+
Контрольний дзвінок	-	-	-	-
Виробник	Росія	Україна	Україна	Китай

Таким чином, після огляду існуючої порівняльної таблиці можна виділити наступні ключові моменти, а саме те, що на ринку не представлено ідеальної охоронно-тривожної системи з відповідним функціоналом і прийнятною ціною, тому доцільність розробленого пристрою не викликає сумніву. Також до системи планується додати набір інтелектуальних правил, які будуть визначати рівень загрози і автоматично вирішувати про уведення адміністративної групи системи.

#### 1.4 Формалізація вимог та постановка задачі

Системи охоронно-тривожної сигналізації є достатньо ефективними для охорони периметру будівлі. Такі системи мають значні переваги в плані швидкодії повідомлення, різноманітному набору давачів для контролю абсолютно всіх зон, простоті керування. Незважаючи на ці переваги, сучасні виробники значно завищують ціну на дані системи, та попри свою завищену вартість мають досить обмежений функціонал.

На основі вище сказаного, роз по своїй будові буде досить простою, що значно скоротить бюджет та час її створення, в той же час, пристрій буде мати широкий функціонал, що закритиме існуючу проблему на ринку.

Опираючись на все це, вимоги до роботи наступні:

- можливість відключення окремих давачів;
- можливість сповіщення при обірвані давачів;
- наявність контролю за тиском;

- наявність контролю за розбиттям скла;
- наявність груп адміністрування;
- наявність правил розподілу адміністрування;
- наявність профілів захисту системи;
- інтелектуальний режим роботи системи;
- невисока вартість системи;
- простота в користуванні системою.

Мікроконтролер повинен бути запрограмований так, щоб при спрацюванні різних давачів (шуму, вібрацій, руху, тиску чи відкриття дверей) сигналізація повідомила про це власника та ввімкнулась сирена.

Для виконання даних вимог для реалізації апаратної частини було обрано платформу Arduino, оскільки дана платформа дозволяє швидко та якісно створити пристрій з можливістю тестування в реальних умовах, а ціна системи буде значно нижча в порівнянні з конкурентами. Дана платформа дозволяє вирішити питання реалізації комплексного захисту, потужності якої вистачить для промислового підприємства.

Даний вибір компонентів надасть змогу розробити систему охоронно-тривожної сигналізації на основі GSM-модуля, більш функціональною, ніж аналогічні системи на ринку, але значно зменшить її вартість.

В даному розділі було проведено аналіз існуючих пристроїв оповіщення. Також розглянуті всі види систем оповіщення, розглянуто їх класифікацію і порівняно пристрій з існуючими аналогами на ринку. В результаті отримано вимоги до розробляючого пристрою, обрано платформу для розробки та задано основні критерії функціональності розробляючого пристрою.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ОХОРОННО-ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ**

### **2.1 Аналіз структури підприємства та схема розміщення компонентів пристрою**

Система охоронно-тривожної сигналізації, яка розробляється в даній роботі призначена для складського приміщення підприємства ТОВ «БРІС» ЛТД, що знаходиться за адресом місто Вінниця, вулиця Волошкава, 55.

Наразі на підприємстві ТОВ «БРІС» ЛТД охорона складського приміщення присутня лише у вигляді охоронця, який завжди може піддатись впливу людського фактору, вербування чи інших речей, що значно зможуть знизити ефективність його роботи.

В складському приміщенні зберігаються запчастини до автомобілів та інші витратні матеріали. Регулярно, раз на місяць на підприємство постачаються достатньо дорогі запчастини, які в подальшому розподіляються по області.

Основне призначення охоронної-тривожної сигналізації - виявлення несанкціонованого проникнення у взятому під охорону приміщення, і як наслідок, забезпечення цілісності майна, а також унеможливлення викрадень чи промислового шпигунства. Охоронна сигналізація дозволяє контролювати і повідомляти про такі процеси, які відбуваються в об'єкті, взятому під охорону:

- розбиття вікна, руйнування стін і перекриттів;
- відкриття дверей і вікон;
- пересування людей всередині приміщень;
- підозрілі шуми на об'єкті захисту.

План складського приміщення зображена на рисунку 2.1, де відображено розташування вікон, дверей, розташування полиць з запчастинами та іншими деталями, які зберігаються.

На плані складського приміщення підприємства показано розміщення елементів. В нижній частині розташовані полиці для деталей чи інших запчастин, де між ними знаходяться тумби. На верхній частині зображені полиці по всій довжині стіни, а в кутку від вікна – тумба. Висота полиць складає 2м, висота тумб – 1м. Висота приміщення – 3м. В центрі приміщення розташований стіл для прийому та видачі деталей, а під час прийому важливих запчастин, які будуть розподілені по області вони залишаються на цьому ж столі до їх розподілення, біля нього – робочий стіл, на якому заповнюються накладні прийому та видачі. Основним джерелом загроз потрапляння в приміщення є вікна і двері, зони яких контролюються відповідними давачами

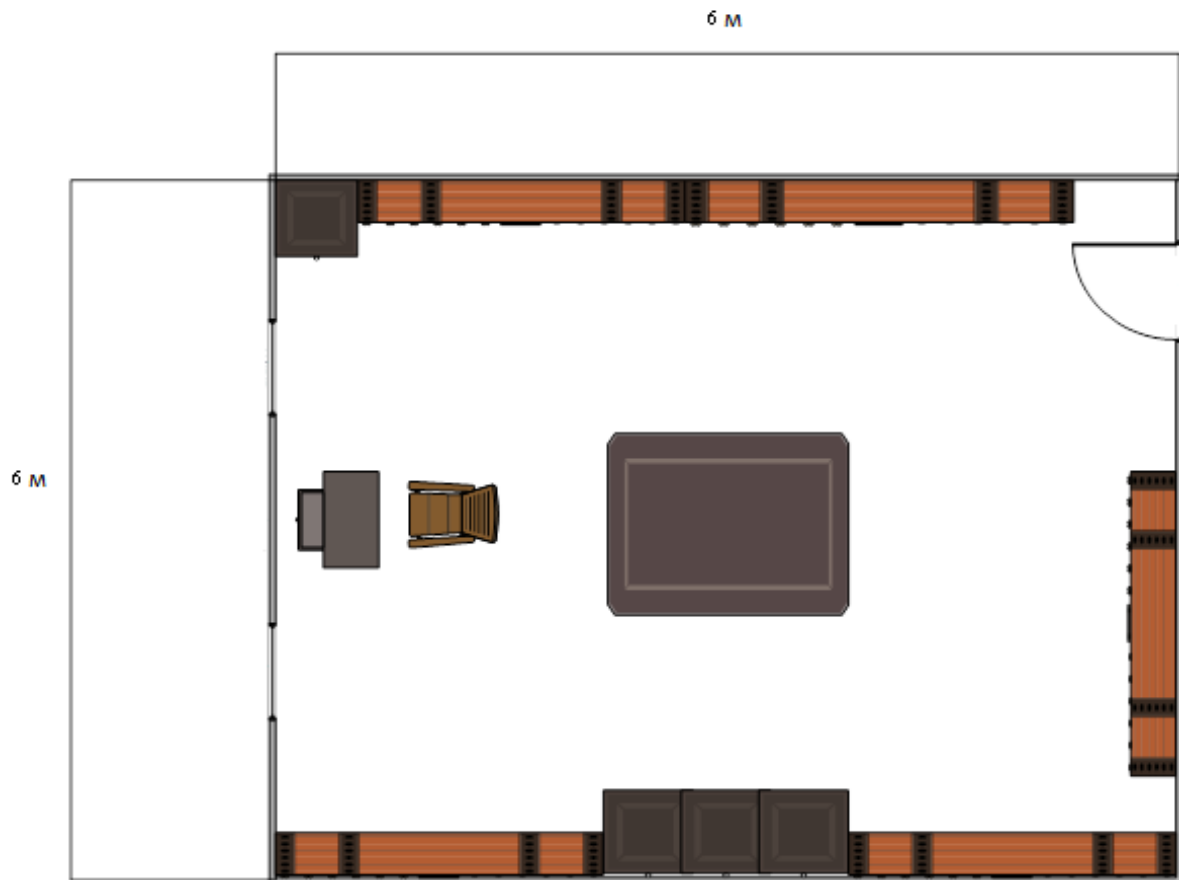


Рисунок 2.1 – План складського приміщення підприємства

Пропонується встановлення датчиків на відповідних позиціях з номерами, де кожен номер це:

- 1 - блок керування;
- 2 - датчик шуму;
- 3 - магнітогерконовий датчик на вікна;
- 4 - датчик руху;
- 5 - магнітогерконовий датчик на двері;
- 6 - датчик удару;
- 7 - ультразвуковий датчик;
- 8 - датчик тиску.

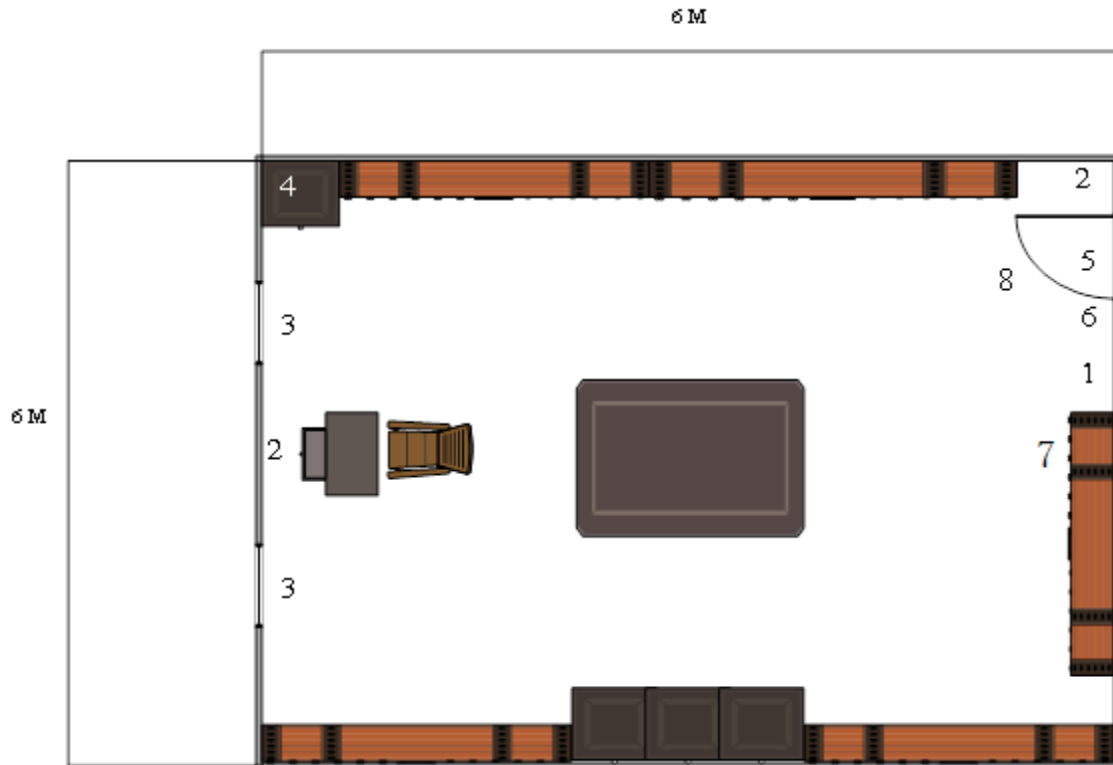


Рисунок 2.12 – Схема розміщення датчиків в складському приміщенні підприємства

Завдяки даному розміщенню датчиків, система повністю контролює сліпі зони приміщення, а зловмисник не зможе потрапити фізично до об'єкта захисту. Варто відмітити, що датчик під номер 7 контролює наявність особливо вартісних запчастин, які поставляються раз на місяць, решта датчиків працюють відповідно до свої контрольованих зон, а саме контроль відкриття дверей, вікон, шуму, руху і вібрацій.

## 2.2 Розробка загальної структури апаратного засобу

Структуру системи охоронно-тривожної сигналізації планується розробити таким чином, щоб забезпечити максимальний захист від несанкціонованого доступу до об'єкту, і щоб досягти цього, слід використати наступні датчики, які будуть покривати всю територію приміщення складу, а саме:

- 1) плата Arduino Nano;
- 2) датчик руху;
- 3) датчик шуму;
- 4) датчик вібрацій;
- 5) магнітний датчик на вікна і двері;
- 6) GSM-модуль;



- 7) контролер напруги;
- 8) акумуляторну батарею;
- 9) давач ультразвуку;
- 10) давач тиску.

Слід виділити останніх два елементи, які покращать захист складського приміщення в повному обсязі. Загальний алгоритм роботи системи охоронно-тривожної сигналізації працює за схемою, яка зображена на рисунку 2.3.

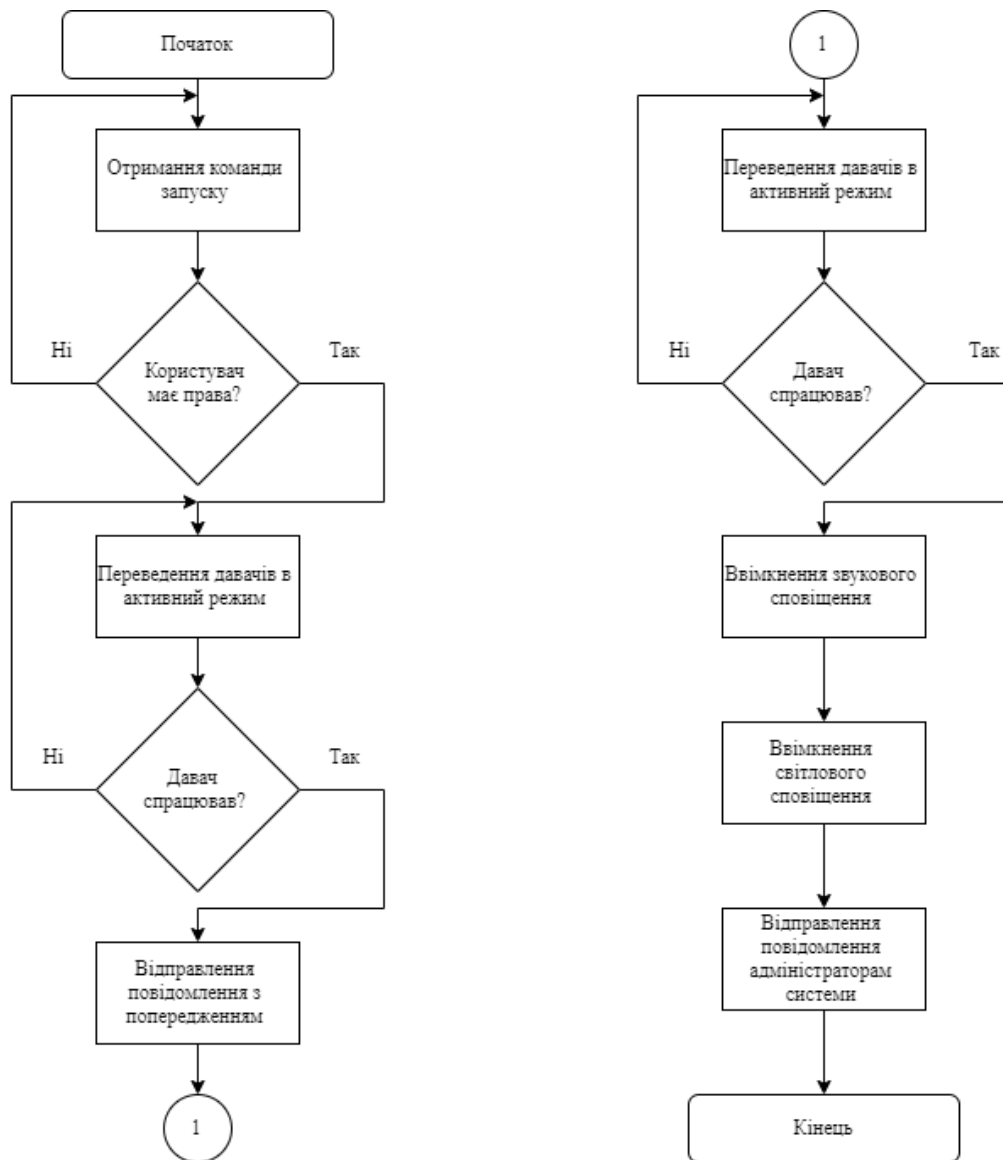


Рисунок 2.3 – Загальний алгоритм роботи системи

При додаванні останніх двох датчиків усі можливі точки входу в приміщення будуть заблоковані, а вийти незаміченим стане неможливим, а у разі проникнення за безпеку приміщення складу будуть відповідати датчик руху,

давач шуму, давач тиску і давач ультразвуку. В сукупності система є достатньо захищеною.

Варто зазначити, що при проектуванні алгоритму роботи системи, було враховано ряд існуючих недоліків в аналогах і додано інтелектуальний режим, який в свою чергу власноруч визначає коли повідомляти адміністратора системи, а коли ні. Алгоритм відключення працює за схемою зображеною на рисунку 2.4

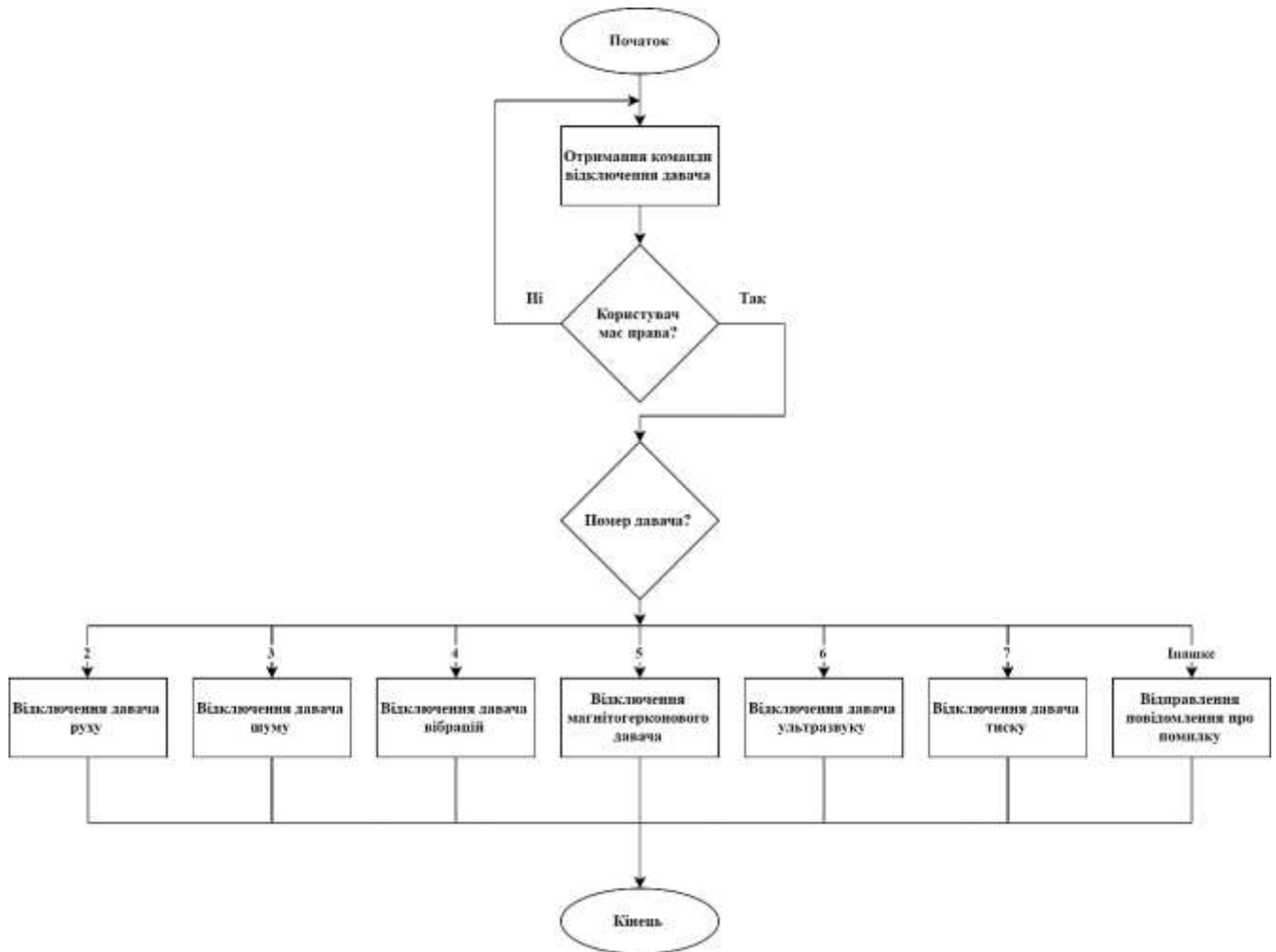


Рисунок 2.4 – Алгоритм відключення датчів охоронно-тривожної сигналізації

Після отримання команди запуску системи від адміністратора, система переводиться в звичайний режим роботи, в якому працюють усі датчів і реєструють усі дії на об'єкті захисту. За замовчуванням вмикаються усі датчів, після чого адміністратор системи може вимкнути окремі датчів відповідними командами в додатку керування або за допомогою SMS команди.

Після спрацювання будь-якого з датчів, надійде SMS повідомлення про те, що було зафіксовано певні дії на об'єкті і одразу ввімкнеться сирена та

світловий сповіщувач. Аналогічно, всі дії та системну інформації можна буде відслідковувати через додаток під ОС Android.

Вимкнути сигналізацію можна за допомогою тумблера, або прибравши живлення чи натиснути відповідну кнопку вимкнення системи на мобільному додатку під ОС Android.

Розглянемо загальну структуру охоронно-тривожної сигналізації, яка розробляється у даній роботі та зображена на рисунку 2.5.

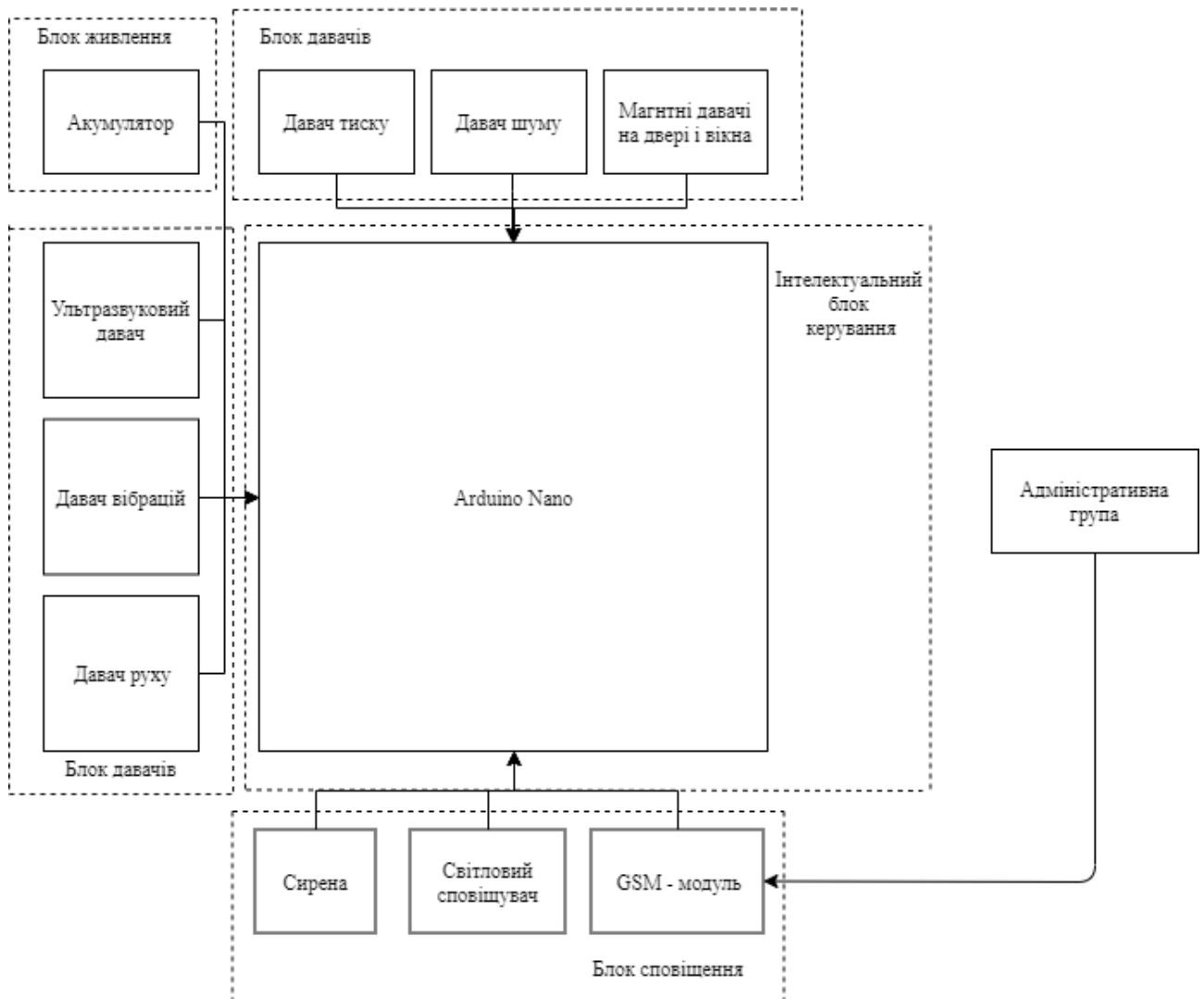


Рисунок 2.5 – Загальна структура системи охоронно-тривожної сигналізації

Блок датчиків призначений для ідентифікації фізичних атак. Кожен з датчиків відповідає за певний вид фізичної атаки, це може бути як і відкриття дверей чи вікон так і рух чи шум на самому об'єкті. Блок живлення відповідає за можливість підзарядки пристрою у екстрених ситуаціях, коли живлення не буде. Блоку сповіщення служить для сповіщення та передачі тривожного

сигналу адміністратору охорони. Блок обробки даних відповідає за взаємодію всіх блоків між собою

Таким чином, можна побачити схожість розробляючого пристрою з типовими охоронно-тривожними системами, оскільки наведено на схемі блоки, які були наведені в першому розділ, проте радикальна різниця між розробляючим пристроєм і аналогами – інтелектуальний блок керування.

Суть роботи інтелектуального блоку починається з того, що у системи є два робочі режими. Звичайний (запускається по команді 1) і інтелектуальний, останній запускається командою 9, і працює за моделлю, яка присвоює кожному з датчиків вагові коефіцієнти, які в свою чергу визначено раніше.

Керувати пристроєм можна як і за допомогою SMS – команд, так і за допомогою додатку, вигляд якого зображений на рисунку 2.6



Рисунок 2.6 – Макет додатку для керування системою

При керуванні пристроєм через додаток, користувач зможе ввімкнути і вимкнути систему відповідними кнопками, а також в поле для виведення інформації буде виводити результат спілкування між системою і користувачем. Таким чином, система буде максимально дружливою до користувача, а її налаштування не займе довго часу.

### 2.3 Інтелектуальний режим системи охоронно-тривожної сигналізації

Інтелектуальний режим роботи системи охоронно-тривожної сигналізації працює на основі вагових коефіцієнтів  $w_i$  для кожного відповідного давача. Перелік усіх можливих коефіцієнтів для кожного з давачів зображено в таблиці 2.1.

Таблиця 2.1 – Вагові коефіцієнти давачів системи охоронно-тривожної сигналізації

№	Давач	Вага параметру
1	Давач руху	0,034
2	Давач шуму	0,033
3	Давач вібрацій	0,033
4	Давач тиску	0,3
5	Ультразвуковий давач	0,3
6	Магнітогерконовий давач	0,3
Всього		1

Вагові коефіцієнти  $w_i$  розставлені за наступною логікою. Давачі під номером 4, 5 і 6 спрацьовують явно на людський фактор, оскільки давач тиску реагує на вагу більшу, ніж 40кг, ультразвуку на явну відсутність предмету і магнітогерконовий давача на явне відкриття дверей чи вікон. Решта давачів можуть спрацьовувати помилково на мілкі об'єкти чи шуми, оскільки технічній частині давачів властиво помилятися навіть після калібрування. Система працює за логікою, де перевіряється сума вагових коефіцієнтів.

$$S_t = \sum_{i=1}^m w_i + S_{t-1} \quad (2.1)$$

Де  $S_t$  – сума вагових коефіцієнтів в момент  $t$ ,  $w_i$  – ваговий коефіцієнт. Принцип роботи є досить простим і ефективним. Кожен давач в такому режимі відправляє на блок обробки даних свої коефіцієнти при своєму спрацюванні. Блок обробки даних в свою чергу при отриманні  $w_i$  починає опитувати інші давачі на предмет спрацювання. Якщо за період в шестидесяти секунд від інших давачів не надійшли данні – блок обробки даних занулює суму і переходить до свого початкового стану, а саме очікує на вагові коефіцієнти.

Розглянемо кожен з можливих випадків і проведемо аналіз реакції інтелектуального блоку на можливі події.

$$S_t = \sum_{i=1}^m w_i + S_{t-1} > 0.29 \quad (2.2)$$

В такому випадку, інтелектуальний блок миттєво оповістить адміністративну групу системи, а саме тих користувачів які можуть корегувати стан системи. Коли ваговий коефіцієнт  $w_i$  більший за показник 0.29 це означає, що найчутливіші давачі явно зреагували на людський фактор. Імовірна похибка такої події досить низька, оскільки ця група давачів явно реагує на людський фактор.

$$S_t = \sum_{i=1}^m w_i + S_{t-1} < 0.29 \quad (2.3)$$

В такому випадку, блок обробки даних почне опитувати всі давачі, на предмет спрацювання і поки ця сума не досягне 0.3 система буде вважати, що це хибне спрацювання давача. Система буде переведена в режим тривоги лише при сумі  $S_t > 0.29$ .

Приклад роботи даного режиму і опис всіх послідовностей зображено на рисунку 2.7.

Вагові коефіцієнти  $w_i$  розподілені таким чином, щоб мінімізувати можливе хибне спрацювання, оскільки давач руху це чутлива система, і явно може зреагувати на подразник у вигляді маленького об'єкту.

На рисунку 2.7 відображено принцип роботи інтелектуального режиму, де:

- D1-D6 – набір давачів відповідно до таблиці 2.1
- S – сума вагових коефіцієнтів  $w_i$
- $W_{D1-D6}$  – ваговий коефіцієнт  $w_i$  відповідно до таблиці 2.1

Нижче, наведено ситуацію, де спрацювали давач руху, давач шуму, давач вібрацій і тиску.

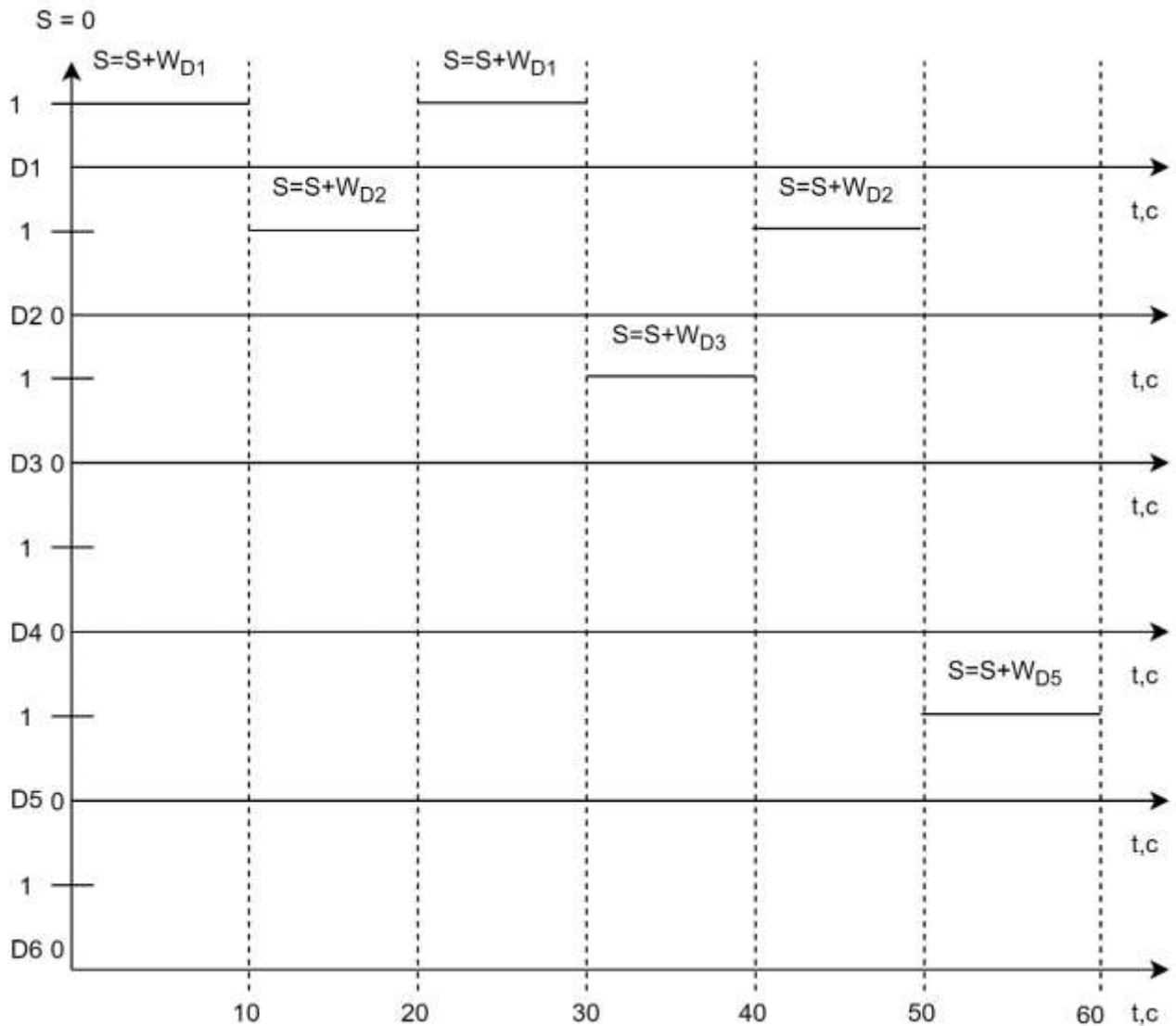


Рисунок 2.7 – Часова діаграма інтелектуального режиму

В цілому варто відзначити, що при розташуванні датчиків, яке було розглянуто у розділі 2.1 при явному несанкціонованому доступі будуть порушені датчики з усіх категорій, тому система чітко спрацює в потрібний момент, і проігнорує можливі похибки.

#### 2.4 Обґрунтування вибору компонентів системи

Система охоронно-тривожної сигналізації, що розроблюється у даній роботі складається з наступних компонентів:

- плата Arduino Nano;
- сирена SHD 4216;
- датчик руху DP-102;
- модуль GSM SIM-800L;

- давач шуму LM-393;
- давач тиску Sparkfun (DAT118);
- давач удару B521;
- магнітний давач DCS-40;
- давач ультразвуку HC-SR04;
- акумулятор.

У якості плати для блоку обробки даних було обрано Arduino Nano, яка зображена на рисунку 2.8.

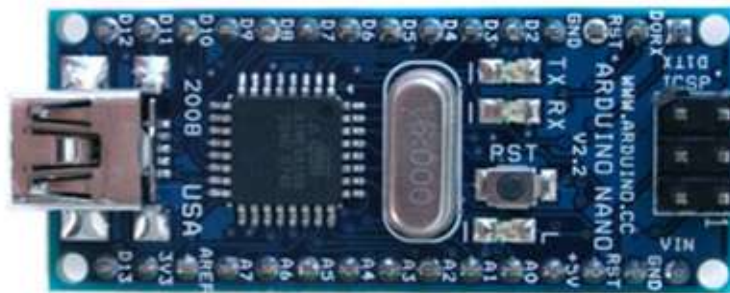


Рисунок 2.8 – Вигляд плати Arduino Nano

Arduino Nano - це функціональний аналог Arduino Uno, але розміщений на мініатюрній платі. Відмінність полягає у відсутності власного гнізда для зовнішнього живлення, використанням чіпа FTDI FT232RL для USB-Serial перетворення і застосуванням mini-USB кабелю для взаємодії замість стандартного. Характеристики [11] даної плати наведені у таблиці 2.2.

Дана плата була обрана через зручність у її програмуванні, та достатню кількість портів для вводу-виводу інформації. Також дана плата містить 8 аналогових входів / виходів, що є зручним для зв'язку.

Модуль звукового сповіщувача SHD 4216 (рис. 2.9) на основі п'єзоелектричного зумера використовується для подачі звукових сигналів тривоги. Даний давач обрано через свою простоту в підключенні, потужність сигналу, яка регулюється та невелику вартість. Також до переваги даної моделі слід віднести невеликі розміри, можливість вибору постійного або перериваючого типу звучання та захищеність від пилу та вологи. Технічні характеристики [11] звукового сповіщувача наведені в таблиці 2.3.

Таблиця 2.2 – Технічні характеристики плати Arduino Nano

Характеристика	Показник
Мікроконтролер	ATmega168 чи ATmega328



## Продовження таблиці 2.2

Робоча напруга	5 В
Напруга живлення (рекомендована)	7-12 В
Напруга живлення (гранична)	6-20 В
Цифрові входи / виходи	14
Аналогові входи	8
Flash-пам'ять	16 КБ чи 32 КБ
SRAM	1КБ чи 2 КБ
EEPROM	512 Б чи 1 КБ
Тактова частота	16 МГц

Також, слід звернути увагу на те, що невеликі розміри модуля звукового сповіщувача дозволять встановити його в важкодоступних місцях, щоб злоумисник не зміг перервати сигнал.

Модуль давача руху DP-102 (рис.2.10) який працює на основі ІЧ пасивного давача обрано через те, що це є найпопулярніший на ринку вид, який широко розповсюджений, має довгий термін роботи, також простота у підключенні до плати Arduino.



Рисунок 2.9 – Модуль звукового сповіщувача

Таблиця 2.3 – Технічні характеристики модуля звукового сповіщувача SHD 4216

Характеристика	Показник
Робоча напруга	3-24 В
Номінальна робоча напруга	12 В
Робочий струм	до 12 мА
Гучність	95 дБ
Частота звуку	3000 ± 500 Гц

Основні технічні характеристики [11] відображені в таблиці 2.4.



Рисунок 2.10 – Модуль давача руху

Даний давач має чудову зону огляду для об'єкта захисту, а також легко калібрується для того щоб уникнути помилкових спрацювань.

Таблиця 2.4 – Технічні характеристики модуля давача руху DP-102

Характеристика	Показник
Зона огляду	До 12 метрів
Номінальна робоча напруга	5-9 В
Область виявлення	110° x 70°

Модуль GSM SIM-800L, відображений на рисунку 2.11, використовується в даній роботі через легке підключення та налаштування, низьке споживання енергії та через сумісність з платою Arduino. Даний модуль чудово зарекомендував себе на ринку і використовується у багатьох виробників охорони-тривожних системах, оскільки він доступний по ціні і має довгий термін роботи [11].



Рисунок 2.11 – Модуль GSM SIM-800L

На таблиці 2.5 відображені основні технічні характеристики [11] даного модуля.

Таблиця 2.5 – Технічні характеристики модуля GSM SIM-800L.

Характеристика	Показник
GPRS class	12
Номінальна робоча напруга	3.7-4.2 В
Підтримка мережі	4х діапазона мережа, 900/1800/1900 МГц
Розміри	25x23мм

Варто відмітити, що завдяки підтримці класу GPRS 12, швидкість передачі даних є вищою, ніж в аналогах, а антена даного модуля дозволяє досить добре приймати мережу.

Давач шуму LM-39 відображений на рисунку 2.12, використовується в проектах, де потрібно вловлювати і вимірювати звукові хвилі [11]. Оскільки на об'єкті захисту слід очікувати підозрілих шумів доцільно використовувати цей давач. В основу роботи давача покладений принцип дії звукових коливань на тонку мембрану мікрофона. Коливання внутрішньої мембрани мікрофону породжують електричні коливання. Напруга, що виникає в процесі роботи давача, подається на інтерфейс для збору даних. На модулі розташований регулятор чутливості. Коли давач уловлює звукові коливання, починає світитися світлодіод, який розташований на його корпусі.



Рисунок 2.12 – Модуль давача шуму LM-39

Даний модуль працює при напрузі 5 В постійного струму. Перевагою даного давача над аналогами є широка розповсюдженість на території України, простота в калібруванні та низька ціна на ринку.

Давач удару B521, який зображений на рисунку 2.13 використовується в основному для систем охоронно-тривожної сигналізації автомобіля [11], але в

даному випадку, доцільно використати його на в даній системі, оскільки можливий механічний вплив як на саму систему, так і на приміщення де вона розташована.



Рисунок 2.13 – Модуль давача удару V521

Основні технічні характеристики [11] давача удару відображені в таблиці 2.6.

Магнітогерконовий давач DCS-40, відображений на рисунку 2.13, пластиковий, накладного типу. Призначений для установки на дерев'яні двері та вікна для контролю стану дверей.

Перевагою даного давача над аналогами є суттєва різниця в ціні, оскільки він базується на простіших принципах, які не поступаються іншим прототипам, а невеликі розміри модуля роблять його встановлення і перебування непомітним для зловмисника.

Таблиця 2.6 – Технічні характеристики давача удару V521

Характеристика	Показник
Робоча напруга	9-15 В
Номінальна робоча напруга	12 В
Робочий струм	до 5 мА
Максимальна робоча температура	85° С
Мінімальна робоча температура	-45° С
Частота звуку	3000 ± 500 Гц
Розмір корпусу	4.2 x 1.6 см

Магнітогерконовий давач є доступною складовою даної системи, який легко знайти на ринку.



Рисунок 2.14 – Модуль магнітогерконового давача DCS-40

Ультразвуковий давач HC-SR04, який зображений на рисунку 2.15 відповідає за контролем особливо важливих об'єктів.



Рисунок 2.15 – Модуль ультразвукового давача HC-SR04

Даний давач, пропонується використовувати, оскільки необхідний контроль за важливими деталями, які регулярно з'являються на об'єкті захисту. Основні технічні характеристики [11] даного давача зображені в таблиці 2.7.

Таблиця 2.7 – Технічні характеристики ультразвукового давача HC-SR04

Характеристика	Показник
Робоча напруга	3.8-5.5 В
Робочий струм	8 мА
Мінімальна дистанція	0 мм
Максимальна дистанція	1500мм

Давач тиску DAT118, який зображений на рисунку 2.16 пропонується використати задля контролю над підлогою приміщення, яка можливо буде піддана несанкціонованому проникненню, оскільки можливий давач добре виконає цю функцію.



Рисунок 2.16 – Давач тиску DAT118

Датчик складається з двох шарів, які розділені спеціальною прокладкою. Чим сильніше ми на нього тиснемо, тим краще стає контакт між напівпровідником. В результаті опір починає зменшуватися і датчик явно показує свій натиск.

Даний давач зміє свій опір залежно від сили, яка додається до нього, відповідно чим більший тиск, тим менший опір. Без тиску опір становить більше 1 МОм. Даний давач фіксує ваги від 30 кг до 95 кг, що безперечно вписується у рамки людського тіла [12].

Також, в роботі пропонується використати акумулятор, ємністю 2800мА, оскільки в сучасній обстановці країни, вимкнення електроенергії є досить частим випадком, а акумуляторна батарея, дозволить використання сигналізації навіть під час таких випадків. Усі давачі і модулі під'єднані до платформи до відповідних їм входів.

Загальна вартість системи складає 940 грн, включаючи захисний корпус, контролер напруги та всі елементи з'єднання, що значно менше ніж виробі з аналогічними характеристиками. У порівнянні з системою Гриф GSM-М (див. табл. 1.2), вартість якої становить близько 2400 грн, дана система коштує майже у 3 рази дешевше. Значна перевага у вартості ґрунтується на компонентах, що використовуються у даному проекті. Дані компоненти є доступними на ринку, та їх налаштування згідно інструкції не займає багато часу.

На рисунку 2.16 відображена схема з'єднань елементів пристрою, на якій відображено електричні зв'язки між структурними елементами даної системи.

За рахунок даного переліку давачів система має значно більший функціонал, при чому її ціна нижча за аналогічні рішення на ринку охоронно-тривожних систем. Внаслідок використання такої кількості давачів, забезпечується максимальна комплексність захисту приміщення об'єкта захисту.

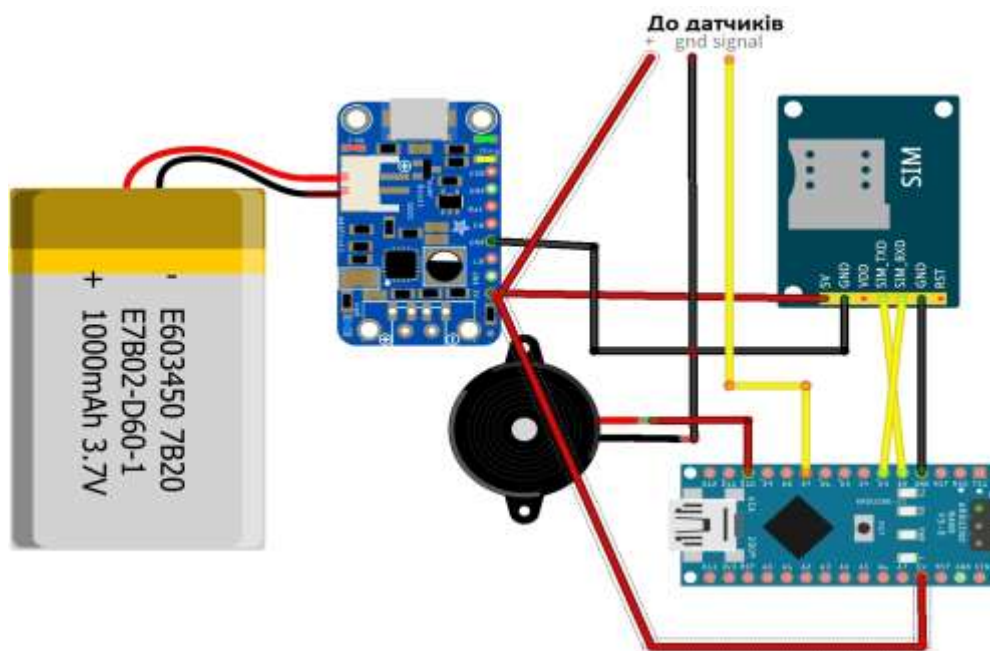


Рисунок 2.16 - Схема з'єднань елементів пристрою

Таким чином, завдяки даній взаємодії елементів системи досягається мета даної роботи. Провівши проектування пристрою, можна переходити до його складання, програмування та тестування, де мусить бути розроблено додаток під операційну систему Android та запрограмовано основний функціонал системи. Результати цих дій відображені в третьому розділі.

## 3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ

### 3.1 Розробка програмної частини системи

Програмна частина для апаратного засобу розроблялась в Arduino Studio, мовою C, оскільки інших компіляторів з таким широким функціоналом немає [13], а мова C є універсальною і яка легко читається та опановується [14]. Спочатку відбувається підключення бібліотек, які відповідають за роботи системи да GSM модуля.

```
#include <SoftwareSerial.h>
#include "Adafruit_FONA.h"
```

Саме для коректного функціонування GSM-модуля, необхідне підключення бібліотеки Adafruit\_Fona.h, а код нижче відповідає з оголошення усіх пінів з датчиками, до яких ми пізніше будемо стукатись.

```
int moveSensor = 5;
int switchPin = 6; //Gercon
int vibrationSensor = 7;
int trigPin = 8;
int echoPin = 9;
int zummerPin = 10;
int voicePin1 = 12;
int voicePin2 = A0;
int powerSensor = A1;
```

При відправленні повідомлення з командою 1, система переводиться в робочий стан, після чого всі фізичні впливи на датчики будуть реєструватись.

```
if (command == 1 && !systemIsWork)
{
    systemIsWork = true;
    sendMessage("SECURITY IS ACTIVE!");
}
```



Завдяки цьому, відбувається підключення і ініціалізація сирени давача руху, шуму, вібрації, магнітогерконового давача та сирени, давача тиску і ультразвуку.

```
int moveSensorData = digitalRead(moveSensor);
if (moveSensorData > 0)
```

В даному прикладі відбувається виставлення умови для спрацювання давача руху, а саме отримання високого сигналу, також можна побачити відповідний ваговий коефіцієнт і інтелектуальний режим системи.

```
intelectualCounter = intelectualCounter + 0.034;
if(intelectualCounter > 0.29 && intelectualMode)
{
    digitalWrite(zummerPin, true);
    sendMessage("MOVING MODULE IS ON! INTELECTUAL ALARM!");
} else if (systemIsWork)
{
    digitalWrite(zummerPin, true);
    sendMessage("MOVING MODULE IS ON! ALARM!");
}
}
```

Після чого система реєструє рух і відправляє SMS повідомлення та вмикає сирену.

```
digitalWrite(zummerPin, true);
sendMessage("MOVING MODULE IS ON! ALARM !");
```

Відбувається виставлення умови для давача шуму, за умовами, що звук буде більше 50 дЦб.

```
int sensorValue = analogRead(voicePin2);
if (sensorValue > 50)
{
    digitalWrite(zummerPin, true);
    sendMessage("NOISE MODULE IS ACTIVE! ALARM!");
}
```

Аналогічним чином запрограмовані всі інші давачі. Наступним чином реалізована інтелектуальний режим роботи системи.

```
intellectualCounter = intellectualCounter + 0.3;
if(intellectualCounter > 0.29 && intellectualMode)
```

Опитуються всі давачі, і перевіряється контрольна сума, якщо вона більша за 0.29 то подається високий сигнал на сирену, якщо ні, сума занулюється через 60 секунд.

### 3.2 Розробка програмної частини додатку для керування системою

Програмна частина для мобільного додатку розроблялась в середовищі Visual Studio Code за допомогою фреймворку для розробки кросплатформених додатків React Native. Даний фреймворк було обрано, оскільки йому притаманний низький поріг входження, а також має широку відкриту документацію [15].

Основою роботи з додатком стала бібліотека для керування SMS – повідомлень з широким функціоналом Get SMS Android, яка в свою чергу містить широкий функціонал фільтрів та яка не займає багато місця і не вантажить систему, на якій буде запущений додаток. Розглянемо функціонал даного додатку.

```
getAllSms(){
  var filter = {
    box: 'inbox',
    // read: 0, // 0 for unread SMS, 1 for SMS already read
    // _id: 1234, // specify the msg id
    address: '+380632754682', // sender's phone number
    // body: 'How are you', // content to match
    // the next 2 filters can be used for pagination
    indexFrom: 0, // start from index 0
    // maxCount: 10, // count of SMS to return each time
  };
```

Дана функція, дозволяє зчитати SMS повідомлення з пристрою в масив, додатково вказавши фільтри, яким в даному випадку служить поле address, де ми обробляємо всі SMS повідомлення від нашої системи.

Надалі ми працюємо з цими даними, і після їх обробки вся інформація потрапляє в вікно логування, де можна побачити всі події, які система зафіксувала.

```

this.state.mailBody.map((item, index) => {return(
  <View style={{borderWidth:2, flexDirection:'row'}}>
    <Text style={{padding:10, fontSize:20,
borderRightWidth:3, paddingRight:10, width: 50, textAlign:
"center"}}>{index+1}</Text>
    <Text style={{fontSize:20, padding:10}}> {item}</Text>
  </View>
)}

```

Керування системою здійснюється за допомогою кнопок, які відправляють повідомлення на систему. Загальний вигляд додатку зображено на рисунку 3.1.

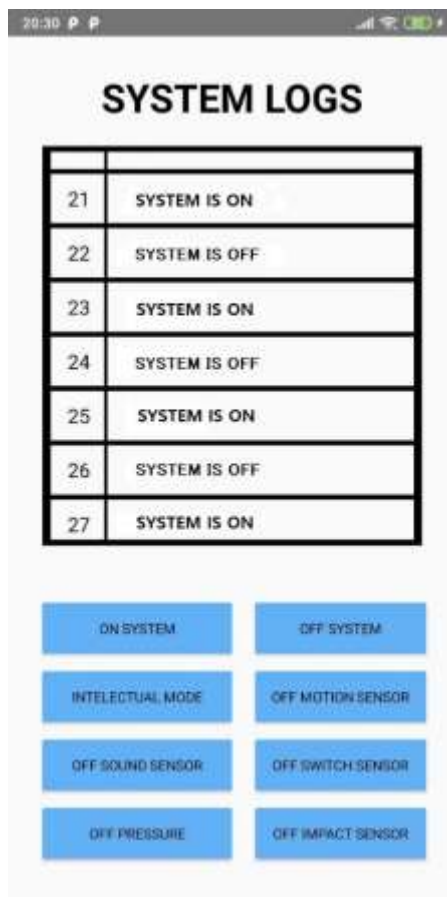


Рисунок 3.1 – Вигляд головного вікна мобільного додатку

Розробивши додаток, можна перейти до його тестування, та до тестування всієї системи в цілому, для перевірки роботи усіх функцій.

### 3.2 Тестування пристрою

Тестування програмної частини апаратного засобу відбувалось в компіляторі Arduino Studio, а саме в його терміналі та паралельно тестувався додаток під ОС Android. Під час тестування проводилась калібрування датчиків руху та шуму на нормальну для людини чутливість, а також підібрано відстані для датчика ультразвуку.

Вигляд системи в зібраному стані зображений на рисунку 3.1. Калібрування датчиків руху і шуму відбувалось за допомогою спеціальних регуляторів, які розташовані на самих датчиках і зображені на рисунку 3.2 і 3.3 відповідно.

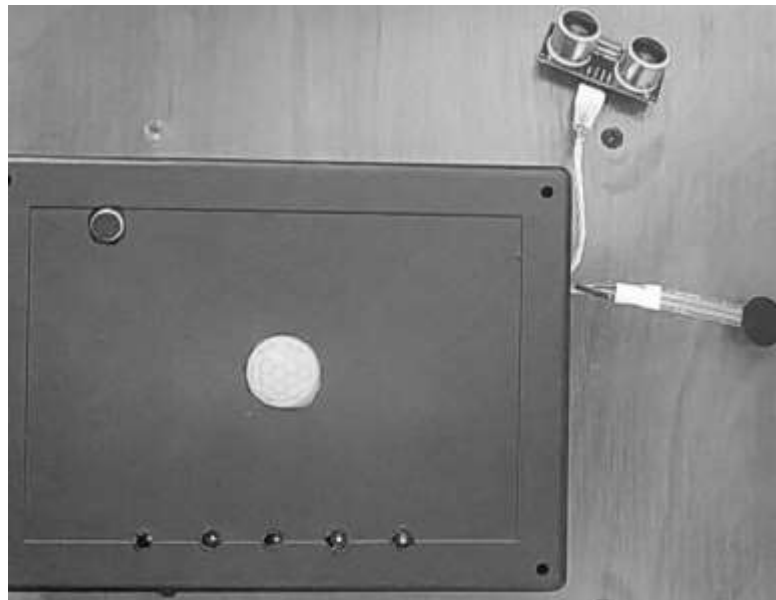


Рисунок 3.1 – Вигляд системи в зібраному стані

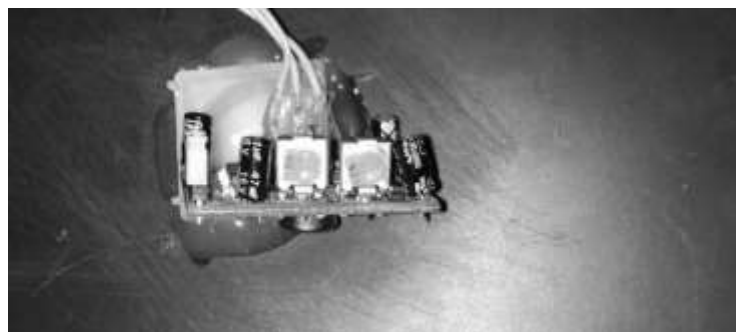


Рисунок 3.2 – Вигляд регуляторів калібрування для датчика руху

Лівий регулятор відповідає за чутливість до руху, а правий безпосередньо за довжину реєстрації. Таким чином можна побачити, що чутливість була відкалібрована на високий рівень, а дальність спрацювання на максимально можливий. Калібрування давача шуму відбувалось за допомогою регулятора, зображеного на рисунку 3.3. Відповідно до цього, давач налаштований на рівень людського голосу, хоча її можна збільшити до рівня крику чи зменшити до рівня шопоту.

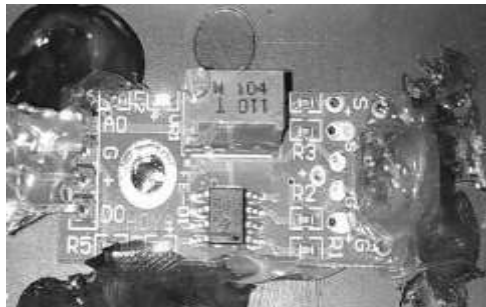


Рисунок 3.3 – Вигляд регуляторів калібрування давача шуму

Вигляд системи в розібраному стані зображений на рисунку 3.4

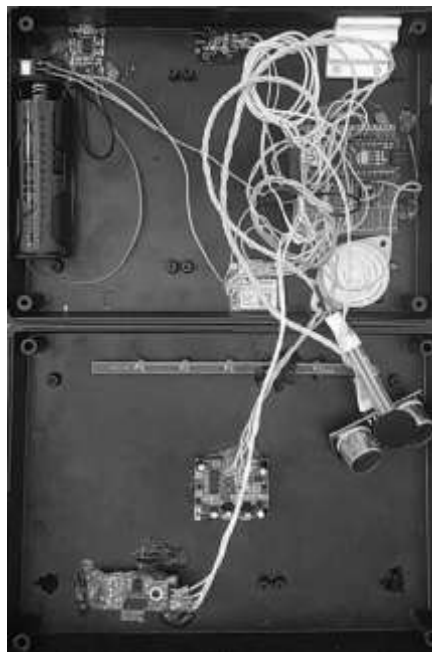


Рисунок 3.4 – Вигляд системи в розібраному стані

Після проведення всіх фінальних налаштувань, було почате тестування системи, навмисно даючи давачам спрацювати.

В результаті було проведено тридцять тестів, п'ять з яких були направлені на давач руху, п'ять на давач шуму, п'ять на магнітогерконовий давач, п'ять на давач вібрацій, п'ять на давач тиску, п'ять на давач ультразвуку. Тести проводились в приміщенні наближеному до об'єкта захисту.

Результатом тестування давача руху стало коректне спрацювання на всіх тестах. Система чітко розпізнає рух та одразу повідомляє про це повідомленням. Результати відображені на рисунку 3.5.

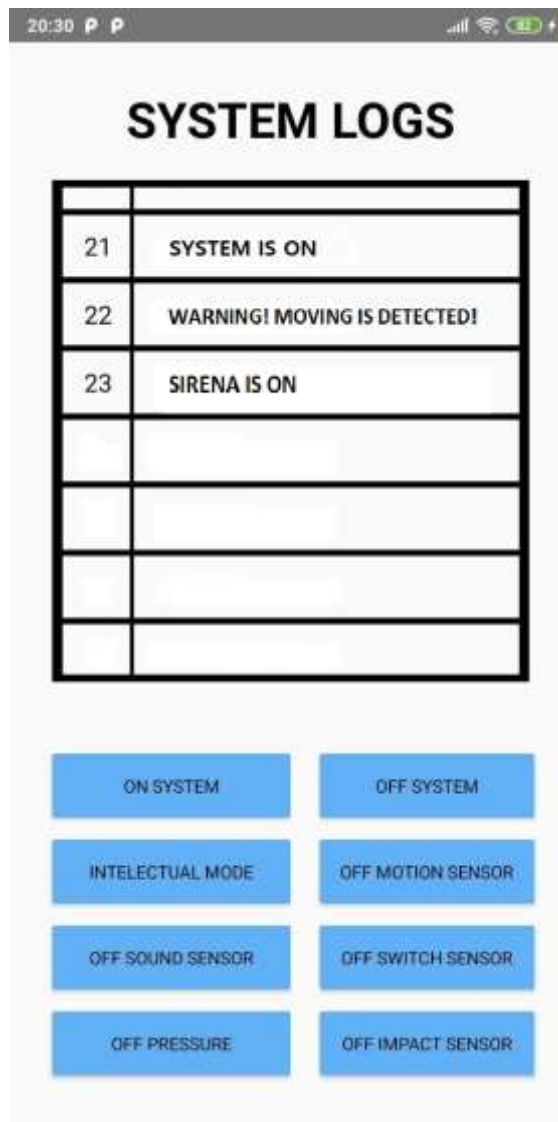


Рисунок 3.5 – Вигляд додатку під час руху

Результатом тестування давача шуму стало коректне спрацювання на всіх тестах. Система чітко розпізнає шум та відкалібрована коректно.

Магнітогерконовий давач на вікна і двері та давач вібрацій також коректно спрацювали на фізичний вплив. Система чітко фіксує кожне відкриття дверей чи вікон, а давач вібрацій розрахований на глибокий шум, що унеможливить укриття фізичного впливу на стіну приміщення. Давач тиску

успішно реагує на вагу понад 30 кілограм а давач ультразвуку успішно реєструє віддалення об'єкту захисту, таким чином можна переконатись в успішності налаштованого пристрою.

За допомогою вище наведених операцій доведено, що даний засіб є доцільним для використання як повноцінна система охоронно-тривожної сигналізації, що сприяє досягненню мети даного проекту.

```
> Security is active!  
^Z  
Sending failed  
  ---> AT+CMGF=1  
  <--- OK  
  ---> AT+CMGD=001  
  <--- OK  
  ---> AT+CMGF=1  
  <--- OK  
  ---> AT+CMGD=001  
  <--- OK  
OK!  
Warning! Noise is detected  
  ---> AT+CMGF=1  
  <--- OK  
  ---> AT+CMGS="+380680051022"  
  <--- >  
> Warning! Noise is detected  
^Z  
Sending failed  
  ---> AT+CMGF=1  
  <--- OK  
  ---> AT+CMGD=001  
  <--- OK  
Sirena is on!
```

Рисунок 3.7 – Вигляд терміналу компілятора під час шуму

Внаслідок проведення тестувань, можна вважати що результат роботи системи є цілком задовільним, а для досягнення більш точних спрацювань потрібно провести повторне калібрування безпосередньо на об'єкті захисту.

## 4 ЕКОНОМІЧНА ЧАСТИНА

### 4.1 Технологічний аудит розробленої інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту

Як було зазначено у попередніх розділах виконаної нами магістерської кваліфікаційної роботи, у зв'язку зі зростаючою кількістю техногенних катастроф, кримінальних та протиправних дій тощо, на перший план в Україні виходять завдання із забезпечення особистої безпеки громадян, а також питання забезпечення безпеки їхнього житла та бізнесу.

Як відомо, загальна стратегія захисту полягає у: а) виявленні несанкціонованого проникнення в приміщення чи виникнення певної небезпечної події; б) локалізації місця і джерела виникнення небезпечної події; в) вчинення дій, що перешкоджають розвитку події; г) документуванні часу, місця і змісту цієї події; д) запровадження заходів щодо усунення самої негативної події або/та її негативних наслідків.

Якщо раніше стратегія захисту будь-якого об'єкта базувалася на організації спеціалізованих служб охорони із залученням великої кількості навчених людей, що здійснювали цілодобове чергування, обходили всі потенційно небезпечні ділянки об'єкта тощо, то сьогодні ця задача розв'язується шляхом застосування різних автоматизованих систем безпеки: сигналізації, відеоспостереження тощо. Сучасні інформаційні технології дозволяють створювати охоронні системи, які своєчасно попереджають їх користувачів про настання або наближення тих чи інших негативних подій.

Разом з тим, велика різноманітність негативних ситуацій, які можуть траплятися у нашому житті, спричинила появу значної кількості систем безпеки і велику кількість рішень, які істотно відрізняються одне від одного як апаратним та програмним забезпеченням, так і пов'язаними з цим функціональними можливостями інформаційних систем, а, відповідно, і їх вартістю.

Тому перед нашою магістерською кваліфікаційною роботою також було поставлене завдання розробити недорогий (бюджетний) апаратно-програмний комплекс, застосування якого дозволило б більш ефективно забезпечувати охорону складських приміщень підприємств. При цьому цей комплекс має мати такий набір давачів, який би забезпечував повний контроль за об'єктом.

Для цього нами було: досліджено та проаналізовано існуючі методи та засоби програмно-технічного захисту; допрацьовано існуючий апаратний засіб шляхом додавання критично важливих давачів та впровадження відповідних логічних і інтелектуальних правил; виконано тестування розробленого



апаратно-програмного засобу; розроблено рекомендації щодо впровадження та експлуатації розробленого програмно-технічного засобу тощо.

У підсумку, нами було розроблено програмно-апаратний засіб, який забезпечує більш високу захищеність підприємства, що має складські приміщення, від зовнішнього фізичного проникнення на його територію за рахунок розробки і використання низки інтелектуальних правил, які дають змогу здійснювати відключення/підключення окремих давачів, забезпечувати оптимальний режим спрацювання системи та можливість роботи з профільними режимами.

Для визначення технічного рівня та комерційного потенціалу нашої розробки проведемо її технологічний аудит. Для проведення технологічного аудиту були запрошені відомі фахівці з цього питання: к.т.н., доцент Куперштейн Л.М., к.т.н., доцентка Войтович Л.П. та ст. викладачка Каплун В.А.

Запрошені до проведення технологічного аудиту експерти здійснювали оцінювання технічного рівня та комерційного потенціалу нашої розробки за методикою та рекомендаціями Державного комітету України з питань науки, інновацій та інформатики [16], які наведено в таблиці 4.1.

Таблиця 4.1 – Критерії оцінювання технічного рівня та комерційного потенціалу будь-якої розробки

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-тері й	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертним висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах

Продовження таблиці 4.1

Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
Ринкові перспективи					
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження таблиці 4.1

Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витратити значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-тері-й	0	1	2	3	4
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промислому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження таблиці 4.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Запрошені експерти проводили технологічний аудит нашої розробки шляхом виставлення оцінок за бальною шкалою (від «0» до «4»; [17]) (дивися таблицю 4.2).

Таблиця 4.2 – Потенційні технічні рівні та комерційний потенціал розробки

Середньоарифметична сума балів $\overline{СБ}$ , розрахована на основі висновків експертів	Технічний рівень та комерційний потенціал розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

В результаті проведеного аудиту експерти виставили нашій розробці такі оцінки, які зведено в таблицю 4.3:

Таблиця 4.3 – Результати технологічного аудиту нашої розробки

Критерії	Прізвище, ініціали експерта		
	Куперштейн Л.М	Войтович Л.П.	Каплун В.А.
	Бали, виставлені експертами:		
1	2	2	3
2	2	2	2
3	2	2	3
4	2	3	2
5	2	3	2
6	2	3	2
7	3	3	3
8	2	2	2
9	2	2	2
10	2	2	2
11	2	2	2
12	2	2	2
Сума балів	СБ <sub>1</sub> =25	СБ <sub>2</sub> =28	СБ <sub>3</sub> =27
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = \frac{\sum_{i=1}^3 СБ_i}{3} = \frac{25 + 28 + 27}{3} = \frac{80}{3} = 26,67.$		

Результати технологічного аудиту та розрахунків, які наведено в таблиці 4.3, показують, що середньоарифметична сума балів, що їх виставили експерти, дорівнює 26,67-ти балам.

Керуючись рекомендаціями, наведеними в таблиці 4.2, можна зробити висновок, що розроблена нами інтелектуальна система охоронно-тривожної сигналізації для промислового об'єкту має технічний рівень та комерційний потенціал, який вважається «середнім».

Це пояснюється тим, що до розробленого нами апаратно-програмного комплексу було додано інтелектуальний режим, який у сукупності з великою кількістю давачів значно підвищує ефективність роботи системи охоронно-тривожної сигналізації із захисту будь-яких промислових об'єктів.

## 4.2 Розрахунок витрат на розробку інтелектуальної системи охоронно тривожної сигналізації для промислового об'єкту

При виконанні даної роботи були використані такі статті витрат [2]: 4.2.1. Основна заробітна плата  $Z_o$  розробників (формула 4.1):

$$Z_o = \frac{M}{T_p} \cdot t \quad \text{грн,} \quad (4.1)$$

де  $M$  – місячний посадовий оклад конкретного розробника;  $U$  ВНТУ місячні оклади коливаються в межах:  $M = (4173 \dots 15500)$  грн/міс.;

$T_p$  – число робочих днів в місяці; прийmemo  $T_p = 25$  днів;

$t$  – число робочих днів роботи розробників.

Розрахунки основної заробітної плати розробників зведено в таблицю 4.4.

4.2.2. Додаткова заробітна плата  $Z_d$  виконавців роботи розраховується як (10...12)% від величини їх основної заробітної плати, тобто:

$$Z_d = \alpha \cdot Z_o = (0,1 \dots 0,12) \cdot Z_o. \quad (4.2)$$

Прийmemo, що  $\alpha = 0,115$ . Тоді для нашого випадку отримаємо:

$$Z_d = 0,115 \times 8701 \approx 1001 \text{ грн.}$$

Таблиця 4.4 – Основна заробітна плата розробників (округлено до цілих чисел)

Найменування посади виконавця	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на оплату праці, грн	Примітка
1. Науковий керівник магістерської кваліфікаційної роботи	11300	452	25 годин	1883	При 36-годинній робочій неділі
2. Студент- магістрант	1940	78	64 день	4992	
3. Консультант з економічної частини	10200	408	2,5 години	170	При 36-годинній робочій неділі
4. Інші фахівці (технолог, інженер)	6900	276	6	1656	
Всього				$Z_o = 8701$ грн	

4.2.3. Нарахування на заробітну плату  $HP_{zp}$  розробників розраховуються за формулою (4.3):

$$H_{\text{зп}} = (3_o + 3_d) \cdot \frac{\beta}{100}, \quad (4.3)$$

де  $\beta = 22\%$  – ставка єдиного внеску на загальнообов’язкове державне соціальне страхування.

Для нашого випадку отримаємо:

$$HP_{\text{зп}} = (8701 + 1001) \times 0,22 \approx 2134 \text{ грн.}$$

4.2.4. Амортизація А основних засобів, обладнання, комп’ютерів тощо розраховується за формулою (4.4) :

$$A = \frac{Ц \cdot H_a}{100} \cdot \frac{T}{12} \text{ грн,} \quad (4.4)$$

де Ц – загальна балансова вартість основних засобів, обладнання, комп’ютерів

тощо, які використовувалися під час виконання роботи, грн;

$H_a$  – річна норма амортизаційних відрахувань. Спрощено можна прийняти, що  $H_a = (5...25)\%$ ;

T – термін, використання кожного виду основних засобів, місяці.

Зроблені розрахунки зведемо у таблицю 4.5.

Таблиця 4.5 – Розрахунок амортизаційних відрахувань

Найменування обладнання, приміщень тощо	Балансова вартість, грн.	Норма амортизації, %	Термін використання, міс.	Величина амортизаційних відрахувань, грн.
1. Обладнання: комп’ютери, принтери тощо	48500	21	3 (40% використання)	1019
2. Приміщення кафедри	15800	4	3 (60% використання)	95
Всього				A = 1114 грн

4.2.5. Витрати на матеріали М:

$$M = \sum_1^n H_i \cdot Ц_i \cdot K_i - \sum_1^n V_i \cdot Ц_v \text{ грн.,} \quad (4.5)$$

де  $H_i$  – витрати матеріалу  $i$ -го найменування, кг;  $Ц_i$  – вартість матеріалу  $i$ -го найменування, грн./кг.;  $K_i$  – коефіцієнт транспортних витрат,  $K_i = (1,1...1,15)$ ;  $V_i$  – маса відходів матеріалу  $i$ -го найменування, кг;  $Ц_v$  – ціна відходів матеріалу  $i$ -го найменування, грн/кг;  $n$  – кількість видів матеріалів.

4.2.6. Витрати на комплектуючі К:

$$K = \sum_1^n N_i \cdot C_i \cdot K_i \quad \text{грн.}, \quad (4.6)$$

де  $N_i$  – кількість комплектуючих  $i$ -го виду, шт.;  $C_i$  – ціна комплектуючих  $i$ -го виду, грн;  $K_i$  – коефіцієнт транспортних витрат,  $K_i = (1, 1 \dots 1, 15)$ ;  $n$  – кількість видів комплектуючих.

Загальна вартість основних матеріалів та комплектуючих, які були використані під час виконання роботи, складає приблизно 1100 грн.

4.2.7. Витрати на силову електроенергію  $V_e$  розраховуються за формулою (4.7):

$$V_e = \frac{V \cdot \Pi \cdot \Phi \cdot K_{\Pi}}{K_d}, \quad (4.7)$$

де  $V$  – вартість 1 кВт-год. електроенергії, в 2019 р.  $V \approx 2,8$  грн/кВт;

$\Pi$  – установлена потужність обладнання, кВт;  $\Pi = 2,32$  кВт;

$\Phi$  – фактична кількість годин роботи обладнання, годин.

Прийmemo, що  $\Phi = 162$  годин;

$K_{\Pi}$  – коефіцієнт використання потужності;  $K_{\Pi} < 1 = 0,83$ .

$K_d$  – коефіцієнт корисної дії,  $K_d = 0,73$ .

Тоді витрати на силову електроенергію становитимуть:

$$V_e = \frac{V \cdot \Pi \cdot \Phi \cdot K_{\Pi}}{K_d} = \frac{2,8 \cdot 2,32 \cdot 162 \cdot 0,83}{0,73} \approx 1197 \quad \text{грн.}$$

4.2.8. Інші витрати  $V_{ін}$  (опалення, освітлення, ремонт, утримання приміщень тощо) розраховуються як (100...300)% від основної заробітної плати розробників, тобто:

$$V_{ін} = (1 \dots 3) \times (Z_o + Z_{роб}). \quad (4.8)$$

Для нашого випадку отримаємо:

$$V_{ін} = 2,00 \times 8701 = 17402 \text{ грн.}$$

4.2.9. Сума всіх попередніх статей дає витрати на виконання роботи безпосередньо магістрантом –  $V_{заг}$ .

$$V_{заг} = 8701 + 1001 + 2134 + 1114 + 1100 + 1197 + 17402 = 32649 \text{ грн.}$$

4.2.10. Загальні витрати на остаточне завершення роботи та оформлення їх результатів розраховуються за формулою (4.9):

$$ЗВ = \frac{V_{заг}}{\beta}, \quad (4.9)$$



де  $\beta$  – коефіцієнт, який характеризує етап виконання даної роботи на шляху до її можливого впровадження. Для нашого випадку доцільно прийняти, що  $\beta$

$$\approx 0,75. \text{ Тоді: } ZB = \frac{32649}{0,75} = 43532,00 \text{ грн або приблизно 44 тисяч грн.}$$

Тобто загальні витрати на остаточне завершення роботи та оформлення її результатів становлять приблизно 44 тис. грн.

### 4.3 Розрахунок економічного ефекту від можливої комерціалізації нашої розробки

Аналіз місткості ринку даної продукції показує, що наразі в Україні кількість потенційних користувачів нашої (або подібної) розробки (а це підприємства, що мають складські приміщення) складає щороку приблизно 1000 осіб і їх кількість буде стрімко зростати (за рахунок значно кращих функціональних можливостей та характеристик нашої системи і прогнозованого рівня зростання злочинності). Тобто, якщо наша розробка буде впроваджена з 1 січня 2021 року (оскільки потребує незначного доопрацювання), то її результати будуть виявлятися протягом 2021-го, 2022-го та 2023-го років.

Прогноз зростання попиту на нашу розробку складає по роках:

- 2021 р. – приблизно + на  $\Delta 300$  шт.;
- 2022 р. – приблизно + на  $\Delta 400$  шт.;
- 2023 р. – приблизно + на  $\Delta 500$  шт.

Якщо існуючі подібні системи охоронно-тривожної сигналізації коштують на ринку в середньому приблизно 5 тис. грн, то нашу розробку можна буде реалізовувати на ринку дещо дешевше, наприклад, за 4,8 тис. грн, чи на 0,2 тис. грн дешевше, що підвищить конкурентоспроможність розробленої нами інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту.

Можливе збільшення чистого прибутку  $\Delta\Pi_i$ , що його може отримати потенційний інвестор від впровадження нашої розробки становитиме [2]:

$$\Delta\Pi_i = \sum_1^n (\Delta\Pi_0 \cdot N + \Pi_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\nu}{100}\right), \quad (4.10)$$

де  $\Delta\Pi_0$  – зміна основного якісного показника від впровадження результатів розробки у цьому році. Таким показником є зміна ціни нової розробки; для нашого випадку це буде:  $\Delta\Pi_0 = (4,8 - 5,0) = -0,2$  тис. грн;

$N$  – основний кількісний показник, який визначає обсяг діяльності у році до впровадження розробки;  $N = 1000$  шт.;

$\Delta N$  – покращення основного кількісного показника від впровадження результатів розробки. Таке покращення відповідно по роках становитиме:

$$\Delta_{21} = +300, \Delta_{22} = +400 \text{ та } \Delta_{23} = +500 \text{ шт.};$$

$\Pi_0$  – основний якісний показник, який визначає обсяг діяльності у році після впровадження розробки; для нашого випадку  $\Pi_0 = 4,8$  тис. грн;

$n$  – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки;  $n = 3$  роки;

$\lambda$  – коефіцієнт, який враховує сплату податку на додану вартість;  $\lambda = 0,8333$ .

$\rho$  – коефіцієнт, який враховує рентабельність продукту. Рекомендується приймати  $\rho = (0,2 \dots 0,5)$ ; візьмемо  $\rho = 0,5$ ;

$\nu$  – ставка податку на прибуток. У 2019 році  $\nu = 18\%$ .

Величина чистого прибутку  $\Delta \Pi_1$  для потенційного інвестора протягом першого року від можливого впровадження нашої розробки (2021 р.) може становити:

$$\Delta \Pi_1 = [-0,2 \cdot 1000 + 4,8 \cdot 300] \cdot 0,8333 \cdot 0,5 \cdot \left(1 - \frac{18}{100}\right) \approx 424 \text{ тис. грн.}$$

Величина чистого прибутку  $\Delta \Pi_2$  для потенційного інвестора від можливого впровадження нашої розробки протягом другого (2022 р.) року може становити:

$$\Delta \Pi_2 = [-0,2 \cdot 1000 + 4,8 \cdot 400] \cdot 0,8333 \cdot 0,5 \cdot \left(1 - \frac{18}{100}\right) \approx 588 \text{ тис. грн.}$$

Величина чистого прибутку  $\Delta \Pi_3$  для потенційного інвестора від можливого впровадження нашої розробки протягом третього (2023 р.) року може становити:

$$\Delta \Pi_3 = [-0,2 \cdot 1000 + 4,8 \cdot 500] \cdot 0,8333 \cdot 0,5 \cdot \left(1 - \frac{18}{100}\right) \approx 752 \text{ тис. грн.}$$

Приведена вартість всіх можливих чистих прибутків ПП розраховується за формулою (в цінах на 1.12.2019 року):

$$\text{ПП} = \sum_{i=1}^T \frac{\Delta \Pi_i}{(1 + \tau)^t}, \quad (4.11)$$

де  $\Delta \Pi_i$  – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої роботи, грн;

$t$  – період часу, протягом якого виявляються результати впровадженої роботи, роки. Для нашого випадку  $t = 3$  роки;

$\tau$  – ставка дисконтування; прийємо ставку дисконтування  $\tau = 0,025$  (2,5%);

$t$  – період часу від моменту здійснення тих чи інших платежів (отримання прибутків та вкладення інвестицій) до моменту впровадження розробки.

Тоді приведена вартість (в цінах на 1.12.2019 року) всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження нашої розробки, складе:

$$\text{ПП} = \frac{424}{(1+0,025)^2} + \frac{588}{(1+0,025)^3} + \frac{752}{(1+0,025)^4} \approx 404 + 546 + 681 = 1631 \text{ тис. грн.}$$

Далі розрахуємо початкову теперішню вартість інвестицій  $PV$ , що можуть бути вкладені інвестором у випадку реалізації нашої розробки:

$$PV = (2 \dots 5) \times 3B, \quad (4.12)$$

де  $3B$  – витрати на розробку;  $3B = 44$  тис. грн (див. формулу 4.9).

Тоді для нашого випадку отримаємо:

$$PV = (2 \dots 5) \times 44 = 4 \times 44 = 176 \text{ тис. грн.}$$

Тоді абсолютний ефект від можливих вкладених інвестицій  $E_{\text{абс}}$  може становити:

$$E_{\text{абс}} = \text{ПП} - PV, \quad (4.13)$$

де  $\text{ПП}$  – приведена вартість всіх можливих чистих прибутків від можливого впровадження нашої розробки, грн;

$PV$  – теперішня вартість інвестицій  $PV = 176$  тис. грн.

$E_{\text{абс}} = 1631 - 176 = 1455$  тис. грн або кожного року приблизно по 485 тис. грн.

Внутрішня норма дохідності  $E_{\text{в}}$  інвестицій, вкладених у комерціалізацію нашої розробки, розраховується за формулою (4.14):

$$E_{\text{в}} = \sqrt[T_{\text{ж}}]{1 + \frac{E_{\text{абс}}}{PV}} - 1, \quad (4.14)$$

де  $E_{\text{абс}}$  – абсолютний ефект вкладених інвестицій;  $E_{\text{абс}} = 1455$  тис. грн;

$PV$  – теперішня вартість початкових інвестицій  $PV = 176$  тис. грн;

$T_{\text{ж}}$  – життєвий цикл розробки, роки.  $T_{\text{ж}} = 4$ .

Для нашого випадку отримаємо:

$$E_{\text{в}} = \sqrt[4]{1 + \frac{1455}{176}} - 1 = \sqrt[4]{1 + 8,267} - 1 = \sqrt[4]{9,267} - 1 = 1,7447 - 1 \approx 0,7447 \approx 74,47 \%$$

Далі визначимо ту мінімальну дохідність, нижче за яку потенційний інвестор не буде займатися комерціалізацією нашої розробки.

Мінімальна дохідність або мінімальна (бар'єрна) ставка дисконтування  $\tau_{\text{мін}}$  визначається за формулою (4.15):

$$\tau = d + f, \quad (4.15)$$

де  $d$  – середньозважена ставка за депозитними операціями в комерційних банках; в 2019 році в Україні  $d = (0,10 \dots 0,19)$ ;

$f$  – показник, що характеризує ризикованість вкладень; зазвичай, величина  $f = (0,05 \dots 0,55)$ , але може бути і значно більше.

Для нашого випадку отримаємо:

$$\tau_{\text{мін}} = 0,15 + 0,52 = 0,67 \text{ або } \tau_{\text{мін}} = 67\%.$$

Оскільки величина  $E_b = 74,47\% > \tau_{\text{мін}} = 67\%$ , то потенційний інвестор може бути зацікавлений у комерційному впровадженні нашої розробки.

Далі розраховуємо термін окупності коштів, які можуть бути вкладені у нашу розробку. Термін окупності  $T_{\text{ок}}$  можна розрахувати за формулою (4.16):

$$T_{\text{ок}} = \frac{1}{E_b}. \quad (4.16)$$

Термін окупності  $T_{\text{ок}}$  коштів, вкладених у нашу розробку, становитиме:

$$T_{\text{ок}} = \frac{1}{0,7447} \approx 1,342 \text{ років,}$$

що свідчить про потенційну доцільність комерціалізації нашої розробки.

Результати виконаної економічної частини магістерської кваліфікаційної роботи зведено у таблицю 4.6:

Таблиця 4.6 – Результати виконаної економічної частини

Показники	Задані у ТЗ	Досягнуті у магістерській кваліфікаційній роботі	Висновок
1. Витрати на розробку інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту	Не більше 50 тис. грн	44 тис. грн.	Виконано
2. Абсолютний щорічний ефект від можливого впровадження розробки, тис. грн	не менше 400 тис. грн за рік	485 тис. грн щорічно протягом 3-х років	Виконано

## Продовження таблиці 4.6

3. Внутрішня норма дохідності вкладених інвестицій, %	не менше 67%	74,47%	Досягнуто
4. Термін окупності, роки	до 3-х років	1,342 років	Виконано

Таким чином, основні техніко-економічні показники розробленої інтелектуальної системи охоронно-тривожної сигналізації для промислового об'єкту, визначені у технічному завданні, виконані.

## ВИСНОВКИ

Задля забезпечення надійного захисту складського приміщення підприємства було проаналізовано основні види охоронно-тривожних систем, які розділяються на чотири групи: охоронно-тривожна сигналізація на основі звукового сповіщувача, сигналізація на основі пульта охорони, система охоронно-тривожної сигналізації з під'єднанням до телефонної лінії та система на основі GSM модуля.

Після проведених досліджень для підвищення стійкості захисту та економічно вигідного впровадження, було прийнято рішення розробити систему охоронно-тривожної сигналізації на основі GSM модуля відмінну від аналогів на ринку наявністю інтелектуального режиму.

Для реалізації засобу на основі аналізу була розроблена структура, яка є удосконаленням загальної типової структури більшості охоронно-тривожних систем, завдяки введенню додавання в її структуру більшої кількості давачів, які будуть охоплювати і контролювати більшу територію, а також розширенням функціоналу.

Було розроблено алгоритм роботи системи та на основі проведених досліджень було обґрунтовано вибір давачів.

Програма для мікроконтролера написана мовою C та змодельована у середовищі Arduino Studio, що дозволило протестувати розроблену систему. Результатом тестування системи стала коректна реакція давачів на відповідні впливи на них.

Перевагами розробленого засобу є простота у використанні, що досягається за рахунок розробленого додатку, можливість забезпечити високий ступінь захисту та економічна доцільність рішення.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тези доповіді [Електронний ресурс] – Режим доступу: URL <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/viewFile/5226/4544> -Назва з екрану.
2. Рынок охранных услуг в Украине [Електронний ресурс] – Режим доступу: URL <https://delo.ua/business/venbest-355468/> - Назва з екрану.
3. Динамика правонарушений в Украине [Електронний ресурс] – Режим доступу: URL <https://delo.ua/economyandpoliticsinukraine/dynamics-of-offenses-in-ukraine/> - Назва з Екрану
4. Барсуков, В. С., Марущенко, В. В., Шигин, В. А. Интегральная безопасность: Информационно-справочное пособие / В. С. Барсуков.–М.: РАО “Газпром”, 2004. – 170 с.
5. Общая теория по охране предприятий и помещений [Електронний ресурс] – Режим доступу URL: <https://www.ritter.kiev.ua/signalizatsia-vse-tonkosti-i-struktura.html> – Назва з екрану.
6. Бузов, Г. А., Калинин, С. В., Кондратьев, А. В. Защита от утечки информации по техническим каналам : Учебное пособие/ Г. А. Бузов. М. : Горячая линия – Телеком, 2005. – 416 с. : ил.
7. Василенок, В. Л. , Вус, М. А., Горшков, В. В. Введение в безопасность предпринимательства : Учебное пособие / В. Л. Василенок– Санкт- Петербург : Высшая административная школа мэрии, 1999. – 99 с.
8. Назначение микроконтроллера в современных системах безопасности [Електронний ресурс] – Режим доступу: URL <http://elektrik.info/main/automation/549-chto-takoe-mikrokontrollery-naznachenie-ustroystvo-princip-raboty-soft.html> – Назва з екрану.
9. Обзор рынка GSM – сигнализаций в Украине [Електронний ресурс] – Режим доступу URL <http://gsm-ukraine.com//rynok-gsm-ohrannyh-sistem/> - Назва з екрану.
10. Дворский, М. Н., Палатченко, С. Н. Техническая безопасность объектов предпринимательства : Учебное пособие / М. Н. Дворский. – М. : А-депт, 2006. – 304 с.
11. Arduino in Ukraine [Електронний ресурс] – Режим доступу URL - <https://arduino.ua/> – Назва з екрану.
12. Тривожная система для умного дома [Електронний ресурс]. – Режим доступу: <http://www.chip-dip.ru/product0/9590.html> – Назва з екрану.
13. Програмування Arduino [Електронний ресурс]. – Режим доступу: URL : [http://academician.kiev.ua/programming\\_in\\_brief.php](http://academician.kiev.ua/programming_in_brief.php) – Назва з екрану.

14. Arduino основи програмування [Електронний ресурс]. – Режим доступу: [http://geekmatic.in.ua/ua/arduino\\_osnovyi\\_programmirovaniya](http://geekmatic.in.ua/ua/arduino_osnovyi_programmirovaniya)– Назва з екрану.
15. React Native – A framework for a building awesome apps [Електронний ресурс]. – Режим доступу: URL <https://facebook.github.io/react-native/> - Назва з екрану
16. Методичні рекомендації з комерціалізації розробок, створених в результаті науково-технічної діяльності – К.: Наказ Державного комітету України з питань науки, інновацій та інформатики (Лист № 1/06-4-97 від 13.09.2010 р.).
17. Козловський В. О. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт. – Вінниця: ВНТУ, 2012.



## ДОДАТОК А

Міністерство освіти і науки України  
Вінницький національний технічний університет  
Факультет інформаційних технологій та комп'ютерної інженерії  
Кафедра захисту інформації

ЗАТВЕРДЖУЮ  
Завідувач кафедри ЗІ д. т. н., проф.  
\_\_\_\_\_ В. А. Лужецький  
\_\_\_\_\_ 2019 р.

### **ТЕХНІЧНЕ ЗАВДАННЯ**

на виконання науково-дослідної роботи

на тему: «Інтелектуальна система охоронно-тривожної сигналізації для  
промислового об'єкту»

08-20.МКР.004.00.000 ТЗ

Керівник магістерської кваліфікаційної роботи  
доц. каф. ЗІ, к.т.н., доц. Л. М. Куперштейн

Вінниця 2019

## **1 Підстави для проведення робіт**

Робота проводиться згідно наказу №254 ректора ВНТУ від 02.10.2019 р.

Дата початку роботи \_\_\_\_\_2019 р.

Дата закінчення роботи \_\_\_\_\_2019 р.

## **2 Мета та призначення НДР**

**Метою** магістерської кваліфікаційної роботи є покращення рівня захищеності від несанкціонованого доступу до приміщення шляхом розробки інтелектуальної системи охоронно-тривожної сигналізації.

**Об'єктом** дослідження магістерської кваліфікаційної роботи є процес контролю доступу до приміщення

**Предмет** дослідження – апаратне та програмне забезпечення системи охоронно-тривожної сигналізації для промислового об'єкту.

**Актуальність теми.** У зв'язку з край нестабільним політичним і економічним кліматом в країні, а також з постійно зростаючою кількістю техногенних катастроф, кримінальних дій, на першому місці виходять завдання з вирішення питань особистої безпеки громадян так і питання безпеки житла, бізнесу. Загальна стратегія захисту полягає в виявленні несанкціонованого доступу до приміщення чи небезпечного події; локалізації місця і джерела події; здійсненні дій, що перешкоджають розвитку події; документуванні часу, місця і змісту події; заходів щодо усунення негативних наслідків події. У минулому стратегія захисту об'єкта базувалася на організації спеціалізованих служб охорони із залученням великої кількості навчених людей, які несли цілодобове чергування, обходили всі потенційно небезпечні ділянки об'єкта, контролювали справність роботи всіх систем і перешкоджали проникненню сторонніх осіб на об'єкт

## **3 Вихідні дані для проведення НДР**

НДР проводиться вперше і вихідними даними для проведення НДР є:

1. Барсуков, В. С., Марущенко, В. В., Шигин, В. А. Интегральная безопасность: Информационно-справочное пособие / В. С. Барсуков.–М.: РАО “Газпром”, 2004. – 170 с.

2. Бузов, Г. А., Калинин, С. В., Кондратьев, А. В. Защита от утечки информации по техническим каналам : Учебное пособие/ Г. А. Бузов. М. : Горячая линия – Телеком, 2005. – 416 с. : ил.

3. Василенок, В. Л. , Вус, М. А., Горшков, В. В. Введение в безопасность предпринимательства : Учебное пособие / В. Л. Василенок– Санкт- Петербург : Высшая административная школа мэрии, 1999. – 99 с.

4. Дворский, М. Н., Палатченко, С. Н. Техническая безопасность объектов предпринимательства : Учебное пособие / М. Н. Дворский. – М. : А-депт, 2006. – 304 с.

#### **4 Виконавці НДР**

Студент групи 1БС-18м Губчакевич Сергій Анатолійович

#### **5 Вимоги до виконання НДР**

##### 5.1 Вимоги до апаратної частини

###### 5.1.1 Варіанти виконання

Пристрій виконується в стаціонарному варіанті, живлення відбувається від блоку живлення.

###### 5.1.2 Контролер пристрою

В якості елемента, що обробляє та видає дані для даного пристрою є плата Arduino Nano.

###### 5.1.3 Обмін даними

Прийом та передача даних пристроєм здійснюється за допомогою GSM-технології.

###### 5.1.4 Режими роботи

- режим сигналізації на основі спрацювань датчиків;
- інтелектуальний режим сигналізації на основі вагових коефіцієнтів.

###### 5.1.4 Керування

Керування режимами роботи пристрою здійснюється за допомогою мобільного додатку для ОС Android.

###### 5.1.5 Індикація

Світлодіодна та звукова індикація роботи пристрою: білий діод, зумер.

###### 5.1.6 Кліматичні умови

Забезпечити стабільну роботу пристрою за умов його експлуатації в температурному діапазоні  $\pm 20^{\circ}\text{C}$ ... $+50^{\circ}\text{C}$  і відносній вологості повітря не більше 75% та тиску – 720-740 мм. рт ст.

###### 5.1.7 Конструктивні вимоги

Пристрій виконується у вигляді окремого функціонального вузла. Маса пристрою не повинна перевищувати 750г, при габаритних розмірах  $160 \times 120 \times 50$ мм.

###### 5.1.8 Вимоги до рівня уніфікації та стандартизації

При розробці пристрою слід максимально використовувати стандартні і уніфіковані деталі.

##### 5.2 Вимоги до програмної частини

### 5.2.1 Вимоги до функціональних характеристик:

- програма повинна виконувати функції контролю доступу до приміщення;
- вхідні дані повинні бути підготовлені у вигляді сигналів від датчиків;
- вихідними даними повинні бути сигнали для ввімкнення охорони;

### 6 Вимоги до супровідної документації

Графічна та текстова документація повинна відповідати діючим стандартам України

### 7 Етапи НДР

Зміст етапу	Початок	Закінчення	Очікувані результати	Звітна документація
Аналіз завдання. Вступ	03.09.19	06.09.19	Вступ	Чернетка вступу
Розробка технічного завдання	09.09.19	15.09.19	Технічне завдання	Проект технічного завдання
Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	16.09.19	12.10.19	Аналіз існуючих аналогів. Вибір напрямку дослідження. Постановка завдання	Чернетка першого розділу
Розробка рішень, моделей, алгоритмів	13.10.19	02.11.19	Аналіз відомих моделей. Математична модель контролю та управління доступом. Обґрунтований вибір елементів	Чернетка другого розділу
Практична реалізація, моделювання, експериментування, результати	03.11.19	20.12.19	Алгоритм функціонування. Показники надійності. Комплексне тестування	Чернетка третього розділу
Розробка економічного розділу	05.12.19	07.12.19	Економічні показники дослідження	Чернетка 3 економічного розділу
Оформлення пояснювальної записки	08.12.19	09.12.19	Пояснювальна записка	Пояснювальна записка

### 8 Очікувані результати та порядок реалізації НДР

Передбачається розробка нової (удосконалення існуючих) охороно-тривожних систем, які спрямовані на покращення рівня захисту від несанкціонованого доступу до нього. Заплановане створення макету засобу, який може бути використаний у навчальному процесі.

## **9 Матеріали які подаються після закінчення НДР**

По завершенню роботи подається пояснювальна записка та ілюстративна частина.

## **10 Порядок приймання НДР та її етапів**

Апробація на науково-технічних конференціях та семінарах. Результати роботи будуть розглядатися на засіданні ДЕК із захисту магістерських кваліфікаційних робіт.

Попередній захист та доопрацювання МКР \_\_\_\_\_2019 р.

Представлення МКР до захисту \_\_\_\_\_2019 р.

Захист МКР \_\_\_\_\_2019 р.

## **11 Вимоги до розроблення документації**

Документація буде виконуватись за допомогою комп'ютерного набору у відповідності вимог ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»

## **12 Вимоги щодо технічного захисту інформації з обмеженим доступом**

У зв'язку з тим що дана робота не містить інформації, що потребує захисту у відповідності до законів України, заходи з її технічного захисту не передбачаються.

## ДОДАТОК Б

### Лістинг апаратної частини

```
#include <SoftwareSerial.h>
#include "Adafruit_FONA.h"
#include <string.h>
#define FONA_RX 2
#define FONA_TX 3
#define FONA_RST 4
int moveSensor = 5;
int switchPin = 6; //Gercon
int vibrationSensor = 7;
int trigPin = 8;
int echoPin = 9;
int zummerPin = 10;
int voicePin1 = 12;
int voicePin2 = A0;
int powerSensor = A1;

char smsbuffer[160];
char PowerOFF[] = "Sirena is off";
char sirena[] = "Sirena is on!";
char sms1[] = "Warning!!! Moving is detected";
char smsW[] = "Security is active!";
char sendsms[160];
String phoneNumber = "+380680051022";

Adafruit_FONA fona = Adafruit_FONA(FONA_RST);
SoftwareSerial fonaSS = SoftwareSerial(FONA_TX, FONA_RX);
SoftwareSerial *fonaSerial = &fonaSS;

void setup()
{
```

```

pinMode(zummerPin, OUTPUT);
// pinMode(vibrationSensor, OUTPUT);
pinMode(switchPin, INPUT);
pinMode(voicePin2, INPUT);

Serial.begin(115200);
pinMode(moveSensor, INPUT);

pinMode(trigPin, OUTPUT);
pinMode(echoPin, INPUT);
pinMode(powerSensor, INPUT);

fonaSerial->begin(4800);
if (!fona.begin(*fonaSerial))
{
    Serial.println(F("Couldn't find FONNA"));
    while (1)
        ;
}
Serial.println(F("FONA is OK"));
Serial.print(F("Found "));
sendMessage("SYSTEM IS ON");

for (int i = 0; i < 100; ++i)
{
    fona.deleteSMS(i);
}
}

bool isFirstCheckDistanceSensor = true;
bool isFirstVoiceSensor = true;
bool isSrenaOn = false;

```

```

int defaultDistance = 0;
int defaultVoice = 0;
float intellectualCounter = 0;
bool systemIsWork = false;
bool intellectualMode = false;
char replybuffer[255];
void loop()
{
    delay(1000);
    retrieveSMS();
    if (systemIsWork)
    {
        checkGerkon();
        checkMoveSensor();
        checkDistanceSensor();
        checkFSRSensor();
        checkVoiceSensor();
    } else if (intellectualMode)
    {
        checkGerkon();
        checkMoveSensor();
        checkDistanceSensor();
        checkFSRSensor();
        checkVoiceSensor();
    }
}

void retrieveSMS()
{
    // Retrieve SMS value.
    uint16_t smslen;
    if (!fona.readSMS(1, replybuffer, 250, &smslen))

```



```

{ // pass in buffer and max len!
    Serial.println("Failed!");
}
Serial.println(replybuffer);
int command = atoi(replybuffer);
if (command == 1 && !systemIsWork)
{
    systemIsWork = true;
    sendMessage("SECURITY IS ACTIVE!");

} else if (command == 9 && !intellectualMode)
{
    intellectualMode = true;
    sendMessage("INTELECTUAL MODE IS ON!");

} else if (command == 2){
    checkMoveSensor(false);
} else if (command == 3){
    checkVoiceSensor(false)
} else if (command == 4){
    checkVibrSensor(false)
} else if (command == 5){
    checkFSRSensor(false);
} else if (command == 6){
    checkDistanceSensor(false);
}

}

void checkFSRSensor()

```

```

{
  int fsrReading = analogRead(powerSensor);
  if (fsrReading != 0)
  {
    intellectualCounter = intellectualCounter + 0.3;
    if(intellectualCounter > 0.29 && intellectualMode)
    {
      digitalWrite(zummerPin, true);
      sendMessage("POWER SENSOR IS ON! INTELECTUAL ALARM!");
    } else if (systemIsWork)
    {
      digitalWrite(zummerPin, true);
      sendMessage("POWER SENSOR IS ON! ALARM!");
    }
  }
}

void checkVoiceSensor()
{

  int sensorValue = analogRead(voicePin2);

  if (sensorValue > 50)
  {
    intellectualCounter = intellectualCounter + 0.033;
    if(intellectualCounter > 0.29 && intellectualMode)
    {
      digitalWrite(zummerPin, true);
      sendMessage("NOISE MODULE IS ACTIVE! INTELECTUAL ALARM!");
    } else if (systemIsWork)
    {

```

```

        digitalWrite(zummerPin, true);
        sendMessage("NOISE MODULE IS ACTIVE! ALARM!");
    }

}

}

void checkMoveSensor()
{
    int moveSensorData = digitalRead(moveSensor);
    if (moveSensorData > 0)
    {
        intellectualCounter = intellectualCounter + 0.034;
        if(intellectualCounter > 0.29 && intellectualMode)
        {
            digitalWrite(zummerPin, true);
            sendMessage("MOVING MODULE IS ON! INTELECTUAL ALARM!");
        } else if (systemIsWork)
        {
            digitalWrite(zummerPin, true);
            sendMessage("MOVING MODULE IS ON! ALARM!");
        }
    }
}

void checkDistanceSensor()
{
    digitalWrite(trigPin, HIGH);
    /* Подаем импульс на вход trig дальномера */
    delayMicroseconds(10); // равный 10 микросекундам
    digitalWrite(trigPin, LOW); // Отключаем
    int impulseTime = pulseIn(echoPin, HIGH); // Замеряем длину импульса

```

```

int distance_sm = impulseTime / 58;          // Пересчитываем в сантиметры

if (isFirstCheckDistanceSensor)
{
    isFirstCheckDistanceSensor = false;
    defaultDistance = distance_sm;
}

if (abs(defaultDistance - distance_sm) > 10)
{
    intellectualCounter = intellectualCounter + 0.1;
    if(intellectualCounter > 0.29 && intellectualMode)
    {
        digitalWrite(zummerPin, true);
        sendMessage("DISTANCE MODULE IS ACTIVE! INTELECTUAL ALARM!");
    } else if (systemIsWork)
    {
        digitalWrite(zummerPin, true);
        sendMessage("DISTANCE MODULE IS ACTIVE! ALARM!");
    }
}
}

void sendMessage(String text)
{
    char number[20];
    phoneNumber.toCharArray(number, 20);
    char sms[100];
    text.toCharArray(sms, 100);

    fona.sendSMS(number, sms);
}

```

```
fona.deleteSMS(1);
}

void checkGerkon()
{
  if (digitalRead(switchPin)==LOW)
  {
    intellectualCounter = intellectualCounter + 0.3;
    if(intellectualCounter > 0.29 && intellectualMode)
    {
      digitalWrite(zummerPin, true);
      sendMessage("DOOR OR WINDOWS IS OPEN! INTELECTUAL ALARM! ");
    }else if (systemIsWork)
    {
      digitalWrite(zummerPin, true);
      sendMessage("DOOR OR WINDOWS IS OPEN! ALARM! ");
    }
  }
}

void startSirena()
{
  digitalWrite(zummerPin, isSrenaOn);
}
```

## Лістинг програмної частини

```
import React, { Component } from 'react';
import {
  SafeAreaView,
  StyleSheet,
  ScrollView,
  View,
  Text,

} from 'react-native';
import SmsAndroid from 'react-native-get-sms-android';
import { Button } from 'native-base';

export default class App extends Component {

  constructor(props) {
    super(props);
    this.state = {
      mailBody:[],
    };
  }

  getAllSms(){
    var filter = {
      box: 'inbox', // 'inbox' (default), 'sent', 'draft', 'outbox',
      'failed', 'queued', and '' for all
      // the next 4 filters should NOT be used together, they are OR-ed so
      pick one
      // read: 0, // 0 for unread SMS, 1 for SMS already read
      // _id: 1234, // specify the msg id
    }
  }
}
```

```

    address: '+380632754682', // sender's phone number
    // body: 'How are you', // content to match
    // the next 2 filters can be used for pagination
    indexFrom: 0, // start from index 0
    // maxCount: 10, // count of SMS to return each time
  };

  SmsAndroid.list(
    JSON.stringify(filter),
    (fail) => {
      console.log('Failed with this error: ' + fail);
    },
    (count, smsList) => {
      console.log('Count: ', count);
      var arr = JSON.parse(smsList);
      console.log('Count: ', arr);
      let arrayWithSms = [];
      for (let i = 0; i < arr.length; i++){
        arrayWithSms.push(arr[i].body)
      }
      console.log(arrayWithSms)
      arrayWithSms = arrayWithSms.reverse()
      this.setState({
        mailBody: arrayWithSms
      })
    },
  );
}

componentDidMount(){
  setInterval(()=>this.getAllSms(), 1000);
}

```

```

    // this.getAllSms();
  }

  sendSms(command){
    SmsAndroid.autoSend(
      "+380632754682",
      command,
      (fail) => {
        console.log('Failed with this error: ' + fail);
      },
      (success) => {
        console.log('SMS sent successfully');
      },
    );
  }

  render() {
    return (
      <View style = {{ margin: 30 }}>
        <Text style={{textAlign:'center', fontSize:40, marginBottom:20,
fontWeight:'bold'}}>SYSTEM LOGS</Text>
        <ScrollView style={{marginBottom: 50, height: '50%',
borderWidth:5}}>
          {
            this.state.mailBody.map((item, index) => {return(
              <View style={{borderWidth:2, flexDirection:'row'}}>
                <Text style={{padding:10, fontSize:20, borderRightWidth:3,
paddingRight:10, width: 50, textAlign: "center"}}>{index+1}</Text>
                <Text style={{fontSize:20, padding:10}}> {item}</Text>
              </View>
            )))
          }
        </ScrollView>

```



```
<View style={{flexDirection:'row'}}>
  <View style={{marginBottom: 15, width:'50%'}}>
    <Button block info onPress={()=> this.sendSms()}>
      <Text>ON SYSTEM</Text>
    </Button>
  </View>
  <View style={{marginBottom: 15, width:'45%', marginLeft:20}}>
    <Button block info onPress={()=> this.sendSms()}>
      <Text>OFF SYSTEM</Text>
    </Button>
  </View>
</View>
```

```
<View style={{flexDirection:'row'}}>
  <View style={{marginBottom: 15, width:'50%'}}>
    <Button block info onPress={()=> this.sendSms()}>
      <Text>INTELECTUAL MODE</Text>
    </Button>
  </View>
  <View style={{marginBottom: 15, width:'45%', marginLeft:20}}>
    <Button block info onPress={()=> this.sendSms()}>
      <Text>OFF MOTION SENSOR</Text>
    </Button>
  </View>
</View>
```

```
<View style={{flexDirection:'row'}}>
  <View style={{marginBottom: 15, width:'50%'}}>
    <Button block info onPress={()=> this.sendSms()}>
      <Text>OFF SOUND SENSOR</Text>
    </Button>
  </View>
</View>
```

```

        </View>
        <View style={{marginBottom: 15, width:'45%', marginLeft:20}}>
            <Button block info onPress={()=> this.sendSms()}>
                <Text>OFF SWITCH SENSOR</Text>
            </Button>
        </View>

    </View>
    <View style={{flexDirection:'row'}}>
        <View style={{marginBottom: 15, width:'50%'}}>
            <Button block info onPress={()=> this.sendSms()}>
                <Text>OFF PRESSURE</Text>
            </Button>
        </View>
        <View style={{marginBottom: 15, width:'45%', marginLeft:20}}>
            <Button block info onPress={()=> this.sendSms()}>
                <Text>OFF IMPACT SENSOR</Text>
            </Button>
        </View>
    </View>

</View>

</View>
);
}
}

```

## ДОДАТОК В

ЗАТВЕРДЖУЮ

Керівник автоколони ТОВ «БРІС» ЛТД

Є. П. Пишний

« \_\_\_ » \_\_\_\_\_ 2019 р.

### АКТ

про впровадження результатів магістерської дипломної роботи  
Губчакевича Сергія Анатолійовича  
на тему «Система охоронно-тривожної сигналізації»

Комісія у складі: голова комісії – керівник автоколони ТОВ «БРІС» ЛТД Пишний Є. П., члени комісії: старший механік автоколони М.М. Маленков і диспетчер О. А. Рогальська. – склала цей акт про те, що у ТОВ «БРІС» ЛТД впроваджено результати магістерської роботи Губчакевича С. А.

Впроваджені результати дозволили:

- здійснювати цілодобовий контроль над приміщенням складу;
- здійснювати швидке сповіщення про незаконне проникнення на території об'єкту;
- підвищити надійність підприємства ТОВ «БРІС» ЛТД.

Голова комісії:

Керівник автоколони \_\_\_\_\_ Є. П. Пишний  
(підпис і печатка)

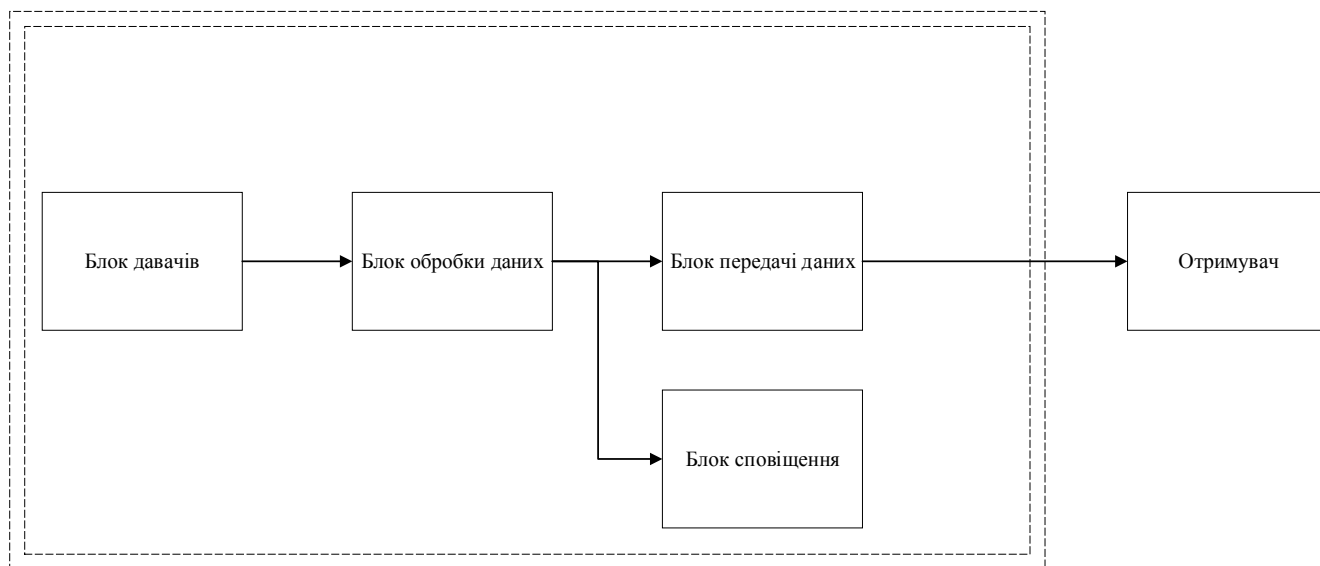
Члени комісії:

Старший механік автоколони \_\_\_\_\_ М.М. Маленков

Диспетчер \_\_\_\_\_ О. А. Рогальська

## ІЛЮСТРАТИВНА ЧАСТИНА

## ТИПОВА СТРУКТУРА ОХОРОННО-ТРИВОЖНИХ СИСТЕМ

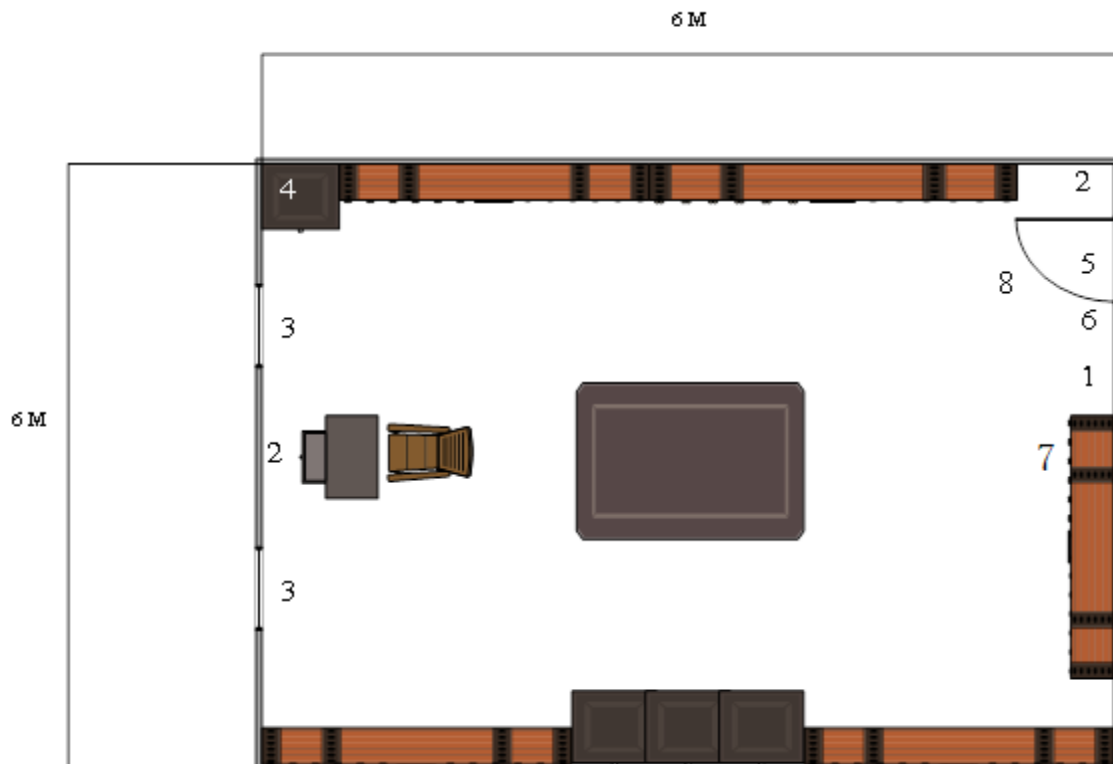


08.20.МКР.004.00.000 ІЧ1

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту. Типова структура охоронно-тривожних систем	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

## СХЕМА РОЗМІЩЕННЯ ДАВАЧІВ В СКЛАДСЬКОМУ ПРИМІЩЕННІ ПІДПРИЄМСТВА

- 1 - блок керування;
- 2 - давач шуму;
- 3 - магнітогерконовий давач на вікна;
- 4 - давач руху;
- 5 - магнітогерконовий давач на двері;
- 6 - давач удару;
- 7 - ультразвуковий давач;
- 8 - давач тиску.

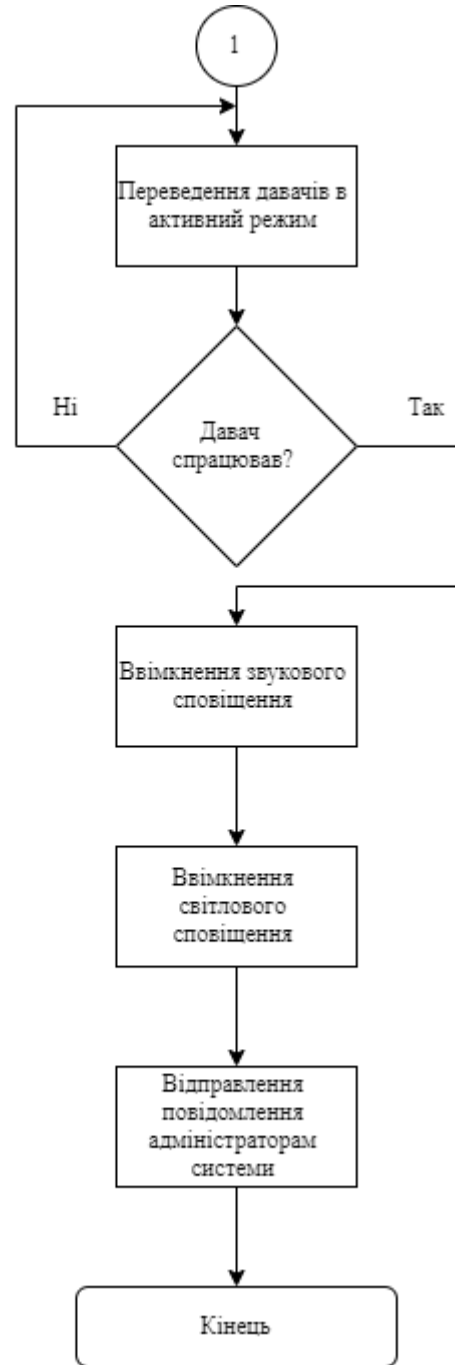
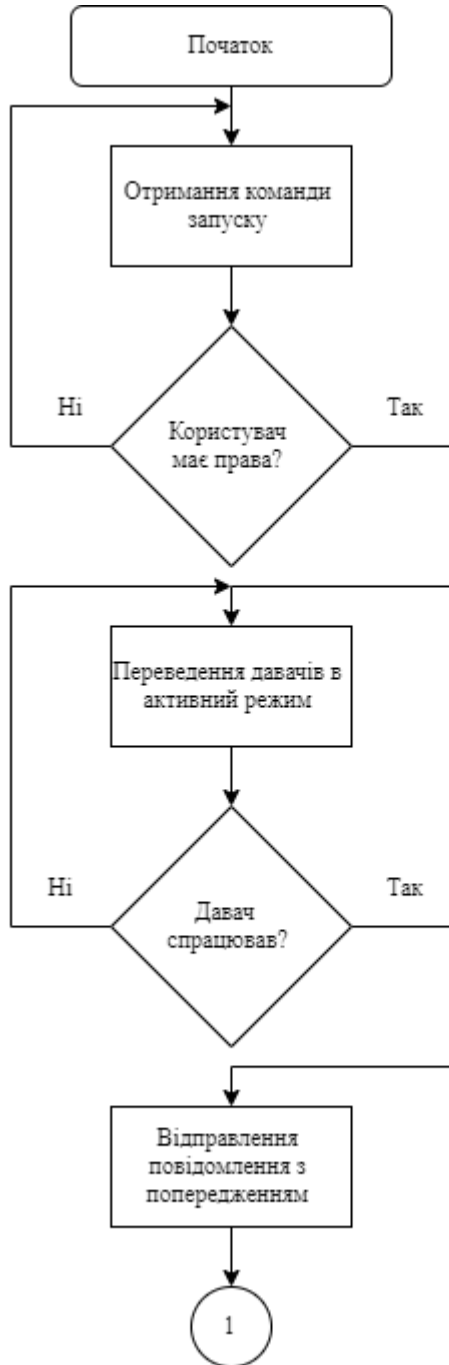


08.20.МКР.004.00.000 ІЧ2

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно- тривожної сигналізації промислового об'єкту. Схема розміщення датчиків в складському приміщенні підприємства	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						



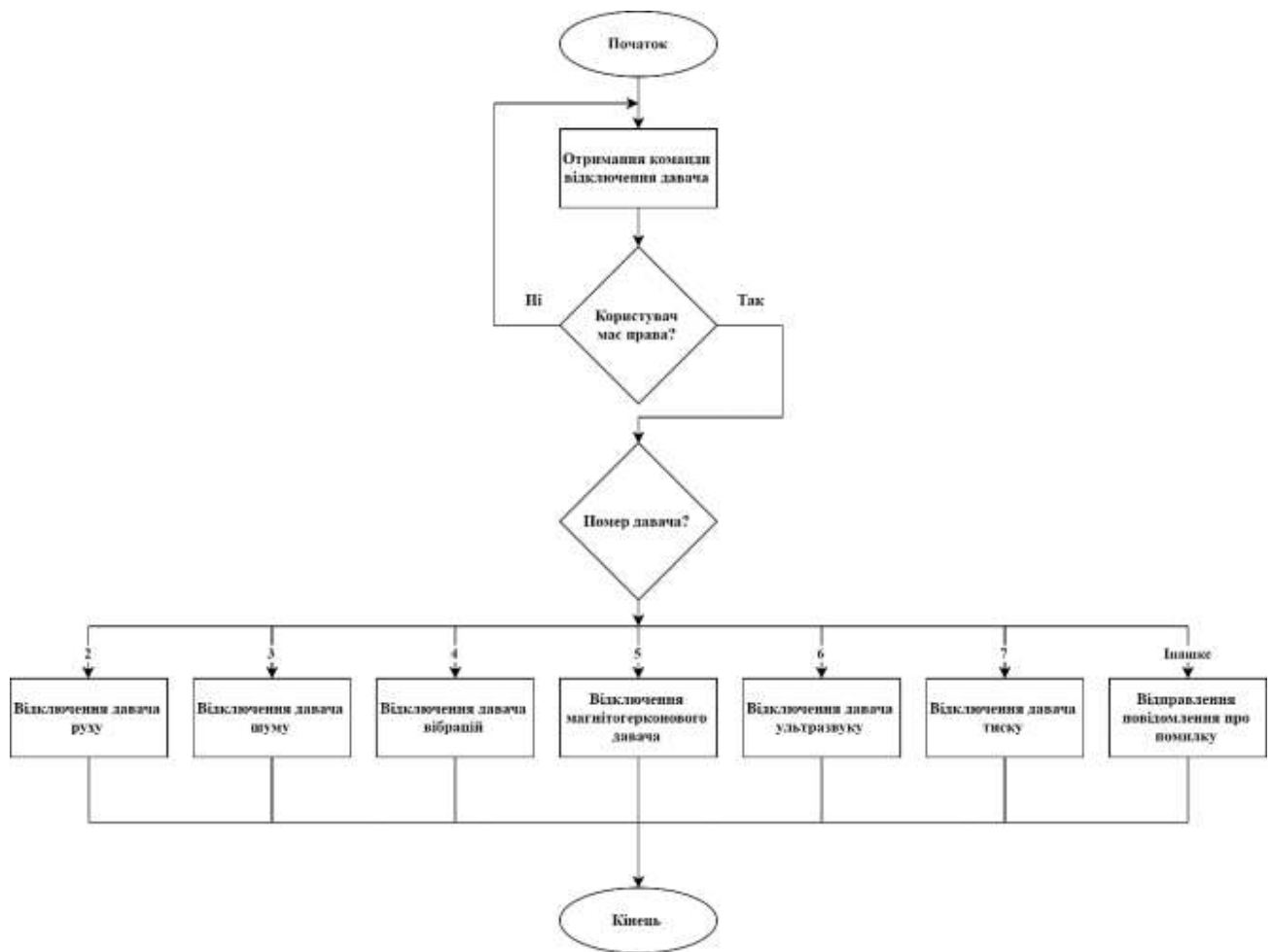
## ЗАГАЛЬНИЙ АЛГОРИТМ РОБОТИ СИСТЕМИ



08.20.МКР.004.00.000 ІЧЗ

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту. Загальний алгоритм роботи системи	Літ.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

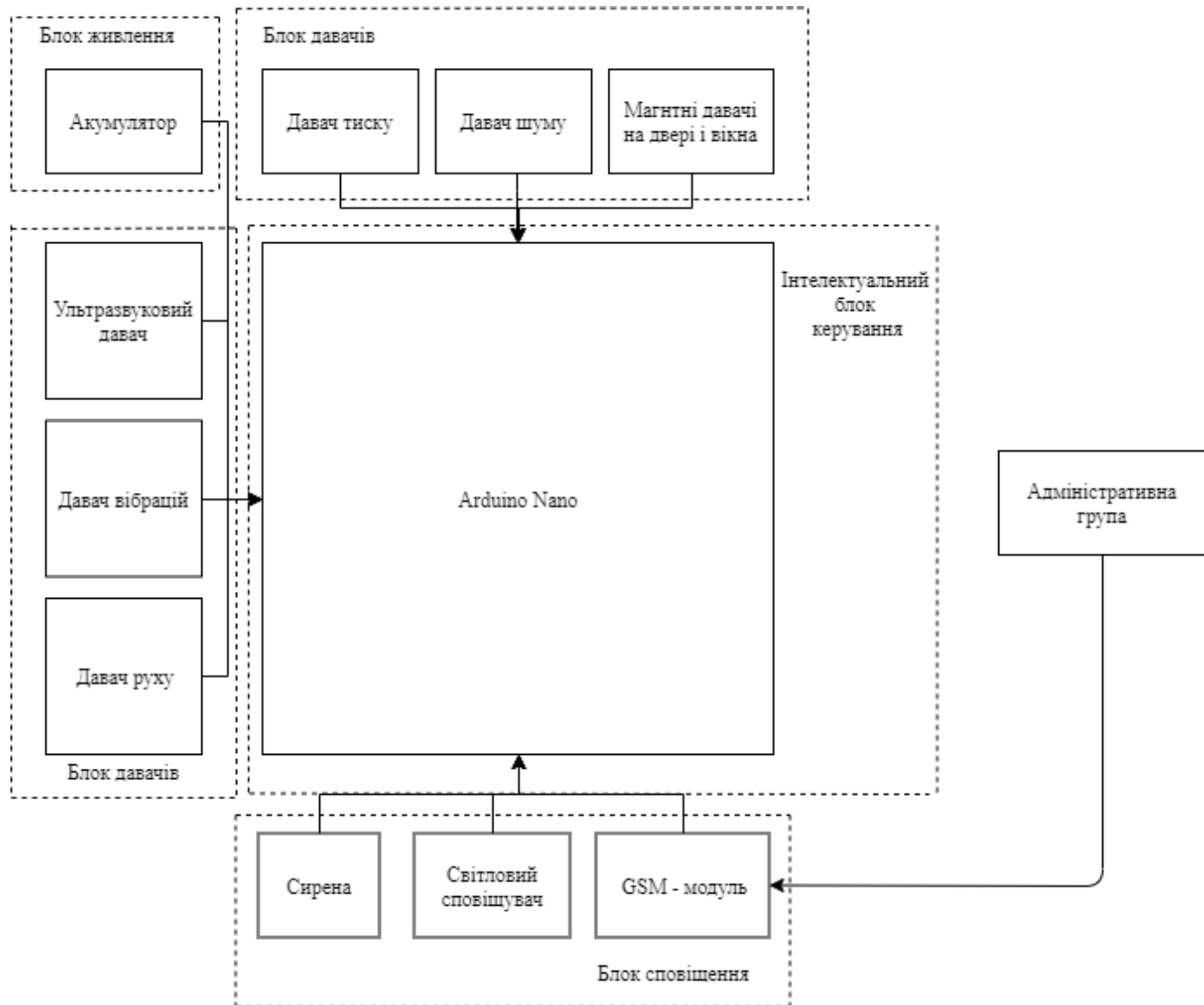
# АЛГОРИТМ ВІДКЛЮЧЕННЯ ДАВАЧІВ ОХОРОННО-ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ



08.20.МКР.004.00.000 ІЧ4

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту. Алгоритм відключення давачів охоронно-тривожної сигналізації	Літ.	Арк.	Аркуші
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

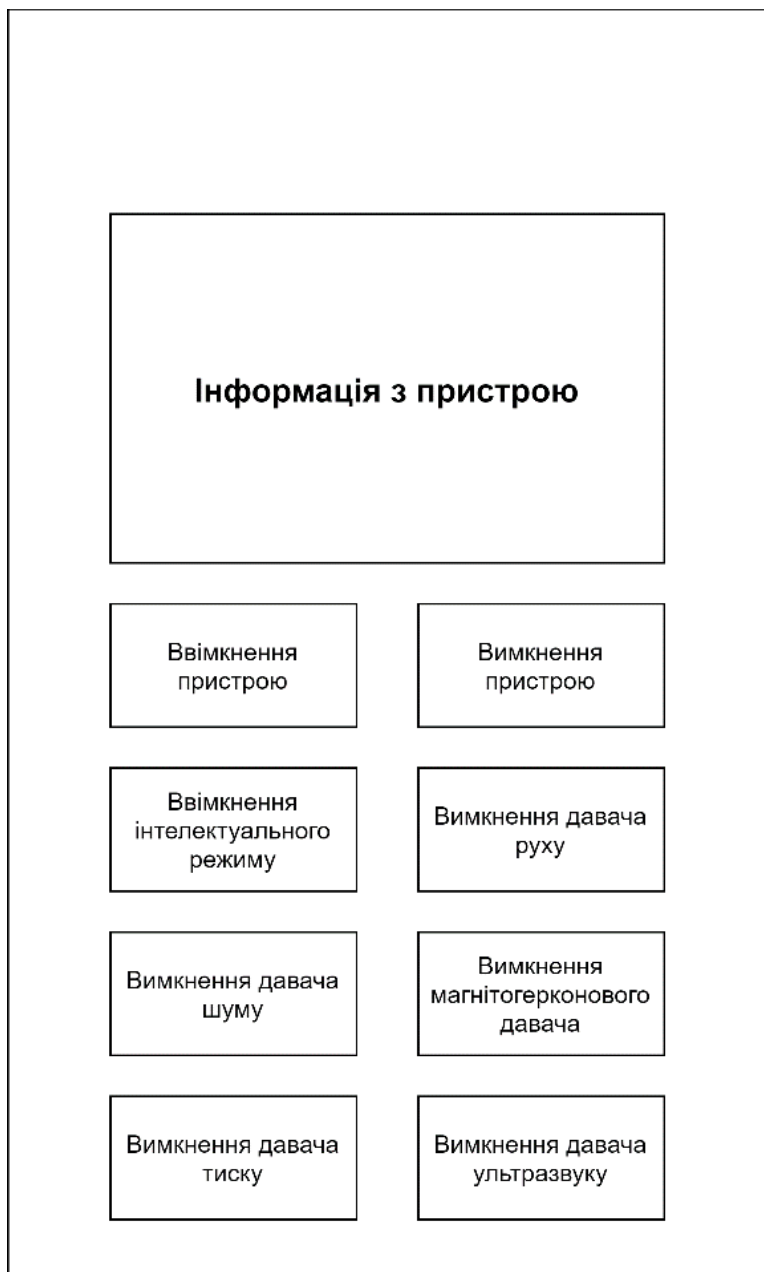
# ЗАГАЛЬНА СТРУКТУРА СИСТЕМИ ОХОРОННО-ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ



08.20.МКР.004.00.000 ІЧ5

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту. Загальна структура системи охоронно-тривожної сигналізації	Лім.	Арк.	Аркушів
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						

## МАКЕТ ДОДАТКУ ДЛЯ КЕРУВАННЯ СИСТЕМОЮ



08.20.МКР.004.00.000 ІЧ6

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Губчакевич С. А.			Інтелектуальна система охоронно-тривожної сигналізації промислового об'єкту. Макет додатку для керування системою	Лім.	Арк.	Аркуші
Перевір.		Куперштейн Л. М.					1	1
Реценз.		Азарова А. О.				ВНТУ, 1БС-18м		
Н. Контр.		Куперштейн Л. М.						
Затверд.		Лужецький В. А.						