МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет мехатроніки та комп'ютерних технологій
(повне найменування інституту, назва факультету)

Кафедра інформаційних та комп'ютерних технологій
(повне найменування інституту, назва факультету)

Дипломна бакалаврська робота
на тему: Автоматизована система контролю доступу до виробничих приміщень

Виконав: студент групи БА-19
Спеціальності:
151 – Автоматизація та комп'ютерно-інтегровані технології
за освітньо-професійною програмою:
Автоматизація та комп'ютерно-інтегровані технології

Костянтин ВІТЕР

Керівник: к.т.н., доц. Юрій ЛЕБЕДЕНКО

Рецензент:_____

Київ 2023

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Інститут, факультет: Мехатроніки та комп'ютерних технологій
Кафедра: Інформаційних та комп'ютерних технологій
Спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані технології
Освітня програма: Автоматизація та комп'ютерно-інтегровані технології

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКТ
доц., к.т.н. Владислава СКІДАН

_____
«___»_____2023 р.

З А В Д А Н Н Я

НА ДИПЛОМНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

ВІТЕРУ Костянтину Максимовичу

1. Тема роботи: Автоматизована система контролю доступу до виробничих приміщень.
   Науковий керівник роботи Лебеденко Ю. О. к.т.н., доц.,
   Затверджені наказом вищого навчального закладу від «08» листопада 2023 року №224-уч
2. Строк подання студентом роботи 19.06.2023 року
3. Вихідні данні до роботи: Система повинна здійснювати контроль доступу до приміщень. А саме надавати доступ до приміщень лише за наявності ключ карти(пропуску), та унеможливлювати доступ до виробничого приміщення сторонніх осіб.
4. Зміст дипломної роботи (перелік питань, які потрібно розробити) Вступ; Розділ 1 Аналіз існуючих засобів для контролю доступу до приміщень; Розділ 2 Розробка апаратної частини контролю доступу до приміщень; Розділ 3 Розробка програмного забезпечення для функціонування системи; Загальні висновки;
5. **Дата видачі завдання:** 08.03.2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної бакалаврської роботи	Термін виконання	Примітка про виконання
1	Вступ	24.04.2023	
2	Розділ 1 Проаналізувати існуючі засоби для контролю доступу до приміщень	01.05.2023	
3	Розділ 2 Розробити апаратну частину контролю доступу до приміщень	10.05.2023	
4	Розділ 3 Розробити програмне забезпечення для функціонування системи	20.05.2023	
5	Висновки	30.05.2023	
6	Оформлення дипломної бакалаврської роботи (чистовий варіант)	01.06.2023	
7	Здача дипломної бакалаврської роботи на кафедру для рецензування (за 14 днів до захисту)	05.06.2023	
8	Перевірка дипломної бакалаврської роботи на наявність ознак плагіату (за 10 днів до захисту)	09.06.2023	
9	Подання дипломної бакалаврської роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	12.06.2023	

Студент _____ Костянтин ВІТЕР
(підпис)

Науковий керівник _____ Юрій ЛЕБЕДЕНКО
(підпис)

Рецензент _____ _____
(підпис)

Директор НМЦУПФ _____ Олена ГРИГОРЕВСЬКА
(підпис)

АНОТАЦІЯ

ВІТЕР К. М. Автоматизована система контролю доступу до виробничих приміщень. – Рукопис.

Дипломна бакалаврська робота за спеціальністю 151 – Автоматизація та комп'ютерно-інтегровані технології. – Київський національний університет технологій та дизайну, Київ, 2023 рік.

Дипломну бакалаврську роботу присвячено розробленню автоматизованої система контролю доступу до виробничих приміщень.

Аналіз технологічного процесу роботи систем сигналізації показав що для покращення ефективності роботи слід правильно обирати датчики враховуючи їх особливості і технічні характеристики. В якості об’єкту керування обрана централь керування(плата Arduino Uno). Проведений аналіз недоліків технологічного процесу.

На основі проведеного аналізу розроблена комп'ютерно-інтегрована, автоматизована система контролю доступу до виробничих приміщень. Вибрано технічну реалізацію комп’ютерно-інтегрованої системи автоматизованого контролю доступу до виробничих приміщень.

Створена система реагування на несанкціоноване проникнення на територію виробничих приміщень, запропоновано алгоритм програми для мікроконтролера.

Ключові слова: сигналізація, комп'ютерно-інтегрована система, автоматичне керування, технологічний процес, контроль доступу до приміщень.

ANNOTATION

VITER K.M. Automated access control system for production premises. - Manuscript.

Bachelor's thesis in the specialty 151 - Automation and Computer-Integrated Technologies. - Kyiv National University of Technologies and Design, Kyiv, 2023.

The bachelor 's thesis is dedicated to the development of an automated access control system for production premises.

The analysis of the technological process of alarm systems revealed that in order to improve efficiency, sensors should be chosen correctly, taking into account their features and technical characteristics. The central control unit (Arduino Uno board) was chosen as the control object. An analysis of the shortcomings of the technological process was conducted.

Based on the conducted analysis, a computer-integrated, automated access control system for production premises was developed. The technical implementation of the computer-integrated system for automated access control to production premises was selected.

A system for responding to unauthorized entry onto the production premises was created, and an algorithm for the microcontroller program was proposed.

Keywords: alarm system, computer-integrated system, automatic control, technological process, access control to premises.

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

GSM – (Global System for Mobile Communications) міжнародний стандарт для мобільного цифрового стільникового зв'язку

PIR – (Passive infrared sensor) пасивний інфрачервоний сенсор

ІЧ – інфрачервоний

LED – (Light Emitting Diode) світловипромінюючий діод

УЗ – ультразвуковий

НВЧ - надвисокочастотні хвилі

МХ – мікрохвильовий

RFID – (Radio Frequency Identification) радіохвильова індентифікація

UID – (Unique Identificator) унікальний ідентифікатор

Бутлоадер – (в перекладі з англійської завантажувач) код що працює при завантажені/запуску

шим-виходи – виходи що підтримують широко імпульсну модуляцію

ICSP - технологія, що дозволяє програмувати електронні компоненти, встановлені в пристрої, системі

UART - тип асинхронного приймача-передавача, компонентів комп'ютерів та периферійних пристроїв, що передає дані між паралельною та послідовною формами

I2C (TWI) - послідовна шина даних для зв'язку інтегральних схем

USB (англ. Universal Serial Bus, універсальна послідовна шина) — стандарт роз'ємів і кабелів для передачі даних

ЗМІСТ

ВСТУП……..…… 9

Розділ 1 Аналіз існуючих засобів контролю доступу до приміщень ……..… 11

1.1 Класифікація…...……..…….…….…. 12

1.2Датчики……..……..……..…….…….. 13

1.3 Герконні датчики…….…… 14

1.4 PIR датчик, або пасивний датчик руху……...……..……..…. 15

1.5 Ультразвукові датчики руху……...…….. 19

1.6 Мікрохвильовий датчик руху……...……..... 20

1.7 Комбіновані датчики руху……..….. 22

1.8 Датчики розбиття скла……...……..….. 22

1.9 Централь…….…….…… 24

1.10 Спрацьовування централі……..……. 24

1.11 GSM модуль …….……...….. 26

1.12 RFID зчитувач ……..…….……...….. 27

1.13 Висновки розділу……...……...….. 29

Розділ 2 Розробка апаратної частини контролю доступу до приміщень..... 30

2.1 Підбір плати(централі)……..….…… 30

2.2 Підбір датчиків……..……..……..….. 32

2.3 Підбір решти складових……..……...…….. 35

2.4 Загальна схема ……...….. 37

2.5 Висновки розділу……..……...……...…….. 38

Розділ 3 Розробка програмного забезпечення для функціонування системи 39

3.1 Опис коду.……..…….…….….. 39

3.2 Висновки розділу……..……...……...…….. 44

Висновки …….……..…….….. 45

Список використаних джерел ……..…….……...…….. 46

Додаток А …….……..…….….. 49

Додаток Б …….……..…….….. 51

Додаток В …….……..…….….. 56

ВСТУП

В сучасному світі, де зростає кількість виробничих підприємств та організацій, забезпечення безпеки приміщень стає все більш актуальною проблемою. Захист від несанкціонованого доступу до важливих приміщень та об'єктів необхідний як для захисту майна, так і для забезпечення безпеки співробітників.

Одним зі способів забезпечення безпеки приміщень є використання автоматизованих систем контролю доступу. Такі системи забезпечують ефективний контроль доступу до виробничих приміщень за допомогою різноманітних технологій, таких як смарт-карти, датчики руху та інші.

Об’єктом дослідження є система автоматичного контролю доступу до виробничих приміщень. Основні методи досліджень це моделювання та експеримент.

Предмет дослідження - методи і засоби побудови автоматизованих систем контролю доступу до виробничих приміщень.

Метою даної роботи є дослідження та розробка автоматизованої системи контролю доступу до виробничих приміщень. **Основним завданням** є створення функціональної системи, яка забезпечує надійний та ефективний контроль доступу до приміщень, що забезпечить збільшення безпеки майна та зниження ризиків несанкціонованого доступу до приміщень та об'єктів.

У роботі були використані наступні методи дослідження:

- емпіричні методи: (експеримент, вимірювання, опис);
- теоретичні методи (аналізу, абстрагування, узагальнення).

Зокрема, застосовано метод декомпозиції для аналізу важливих факторів, що впливають на ефективність роботи системи контролю доступу до виробничих приміщень та методи імітаційного моделювання для підтвердження ефективності результатів роботи системи.

Інформаційна база дослідження: у процесі написання дипломної бакалаврської роботи були використані наукові публікації, що стосуються методів і засобів створення та реалізації комп'ютерно-інтегрованої системи контролю доступу до виробничих приміщень. Ці джерела були отримані з фондів бібліотеки КНУТД та з ресурсів глобальної мережі Інтернет.

Наукова новизна одержаних результатів полягає у вдосконаленні алгоритму роботи та ефективності системи контролю доступу до виробничих приміщень і розробці комп’ютерно-інтегрованої системи автоматизованого керування, яка може бути використана в виробничих приміщеннях для покращення їх захисту.

Апробація результатів бакалаврської роботи: тези доповіді представлені на X Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих вчених з автоматичного управління від 12 квітня 2023 року, Херсон – Хмельницький (Додаток 1) .

Щоб забезпечити коректне функціонування системи необхідно:

- проаналізувати існуючі засоби для контролю доступу до приміщень
- підібрати необхідні комплектуючі (сенсори і датчики)
- розробити апаратну частину контролю доступу до приміщень
- розробити все необхідне програмне забезпечення для функціонування системи

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕНЬ

Система сигналізації - це спеціальна система, яка встановлюється на об'єктах нерухомості, і має на меті сповістити власника або охоронні служби про будь-яке несанкціоноване проникнення на територію об'єкта. Використання системи сигналізації дозволяє суттєво знизити витрати на охорону, завдяки зменшенню кількості необхідного персоналу на кожну одиницю площі об'єкта.

Щоб досягти максимальної ефективності системи сигналізації, потрібно враховувати такі фактори, як наявність входів та виходів на об'єкт, можливі точки проникнення, такі як вікна, вентиляційні отвори, а також особливості будівельного планування та місцевості. Кожен об'єкт має свої особливості, які необхідно враховувати при встановленні системи сигналізації.

Система сигналізації має перший рубіж охорони, який формують віконні та дверні детектори. Магнітоконтактні оповіщувачи спрацьовують, коли двері або вікно відчиняються, і магніт віддаляється на відстань від геркона, замикаючи або розмикаючи контакти. Акустичні детектори реагують на звукові коливання, що виникають при розбитті скла.

Всередині приміщення контролюють об'ємні датчики руху, які аналізують інфрачервоні, електромагнітні або ультразвукові хвилі, відображені від об'єктів. Якщо об'єкт з'являється в полі зору датчика, параметри хвиль змінюються, і це стає приводом для спрацьовування сигналу тривоги.

Центральна система постійно зв'язується з детекторами, отримуючи від них звіти про їх стан і повідомляючи про успішну обробку інформації. Деякі старі моделі мають односторонній зв'язок "датчик→централь", але надійна система моніторить стан оповіщувачів з мінімальними паузами, не перевищуючи 12-15

секунд. Якщо пристрій не відповідає, централь повідомляє користувачеві про несправності в SMS-повідомленні.

1.1 Класифікація

Сучасний ринок систем безпеки пропонує різні типи пристроїв, які можуть бути з широким функціоналом або спеціалізовані для конкретних потреб. Ці системи можуть реагувати на різні фактори ризику і надавати різні типи сигналів в разі небезпеки. Вони можуть бути розроблені для відлякування правопорушників, сповіщення центру управління або виклику поліції. Класифікація таких систем має багато критеріїв, але я розглянув основні види сигналізацій.

1. Залежно від призначення або специфіки об'єкта, що охороняється:
   - для дому (включаючи прибудинкову територію);
   - для квартири;
   - для гаража;
   - для автомобіля;
   - для офісу і т. д.
2. З урахуванням спеціалізації того, що розцінюється такою системою як “небезпека”:
   - охоронна сигналізація від злому (реагує на рух, удари, розбиття вікон);
   - протипожежна система (що повідомляє про задимлення, різкий підйом температури);
   - захист від затоплення (фіксує виникнення протікання в системах опалення та водопостачання);

- захист від чадного газу (що заміряє концентрацію небезпечних речовин у повітрі, може бути частиною протипожежного комплексу);

- універсальна (має на увазі наявність датчиків реагування на всі небезпечні ситуації).

3. За способом передачі тривожного сигналу всередині системи виділяють наступні види сигналізацій для квартири (або будинки):

- провідні (всі повідомлення від датчиків до блоку управління відправляються за допомогою мережі кабелів);
- бездротові (в якості каналів в рамках системи використовуються радіозв'язок або GSM-сигнал);
- гібридні (комбінація двох технологій).

4. Залежно від каналу оповіщення власника про надзвичайну ситуацію існує:

- кабельна система;
- сигналізація на телефон;
- GSM-сигналізація;
- супутникова;
- інтернет-система.

1.2Датчики

Основна задача датчиків в охоронних системах- помітити проникнення на територію охороняємого об’єкту. А будь яке проникнення так чи інакше пов’язане з рухом тому більшість датчиків, що застосовуються в таких системах це датчики руху. А всі відмінності між ними обумовлені місцями в яких вони застосовуються.

1.3 Герконні датчики

Найпростіші датчики руху це герконні датчики, які складаються з двох частин: частини з магнітом і частини з герконом.

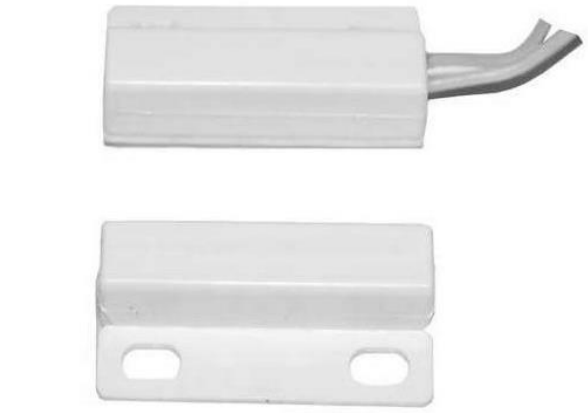


Рис. 1.1 Датчик типу геркон

Геркон - це скляна колба, яка містить металеві контактні пластини. Вони розташовані у паралельних площинах на малій відстані одна від одної, і гнучкі, що дозволяє їм змінювати свою форму в присутності магнітного поля. Герконні датчики складаються з двох частин: одна містить магніт, а інша - геркон. Коли магніт знаходиться в певному положенні, він впливає на контактні пластини геркона, змінюючи їх положення і змушуючи їх замикатись або розмикатись. Таким чином, герконні датчики можуть виявляти наявність або відсутність магнітного поля, що може використовуватись для виявлення руху. Деякі геркони мають

перекидні контакти, які можуть замикати один контакт та розмикати інший залежно від наявності магнітного поля.

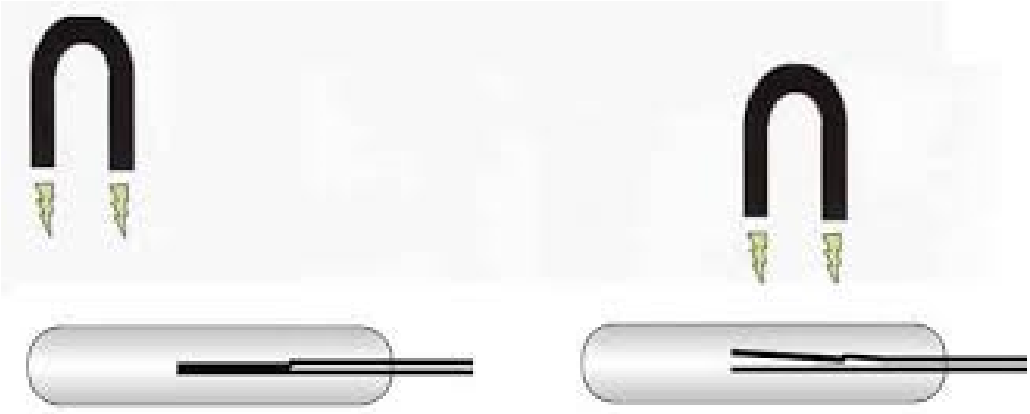


Рис. 1.2 Ілюстрація роботи геркона

Зважаючи на особливості цього типу датчика руху, його встановлюють на вікна, двері та люки (якщо вони є). Він спрацьовує в разі відкриття того, на чому він встановлений, та передає сигнал до централь системи, яка інтерпретує цей сигнал як спробу проникнення на об'єкт.

1.4 PIR датчик, або пасивний датчик руху

Датчик руху, використовуючий технологію піроелектричного ефекту (ПІР), призначений для виявлення руху в заданій зоні контролю. Цей датчик має декілька переваг, таких як компактність, низька вартість, мале енергоспоживання, простота у використанні та високий термін експлуатації. Його можна зустріти під різними назвами, такими як "датчик руху ІЧ", "ПІР датчик", "Пасивний інфрачервоний датчик".

Рис. 1.3(PIR датчик)

В основі датчика лежить піроелектричний кристал, розміщений у металевому корпусі, цей чутливий елемент визначає рівень інфрачервоного випромінювання.

Датчик складається з двох частин, які порівнюють рівень фону з кожної половини датчика під час руху зліва направо, або зправа наліво. Якщо з однієї половини надходить більше сигналу, ніж з іншої, то на виході з'являється сигнал. У звичайному стані потенціали вирівнюються, тому сигнал відсутній. Для підсилення сигналу чутливий елемент має вбудований підсилювач, що складається з резисторів і конденсаторів.

Електронний датчик PIR перетворює вхідний аналоговий сигнал на цифровий вихідний сигнал. Цей тип датчика залишається популярним завдяки своїм споживчим характеристикам. Для більшості продуктів достатньо двох елементів живлення на рік безперервної роботи. Проте важливо пам'ятати, що датчик не може точно визначити, скільки людей перебуває в контрольованій зоні та на якій відстані вони знаходяться від датчика.

Для покращення характеристик ІЧ-датчика, виробники випускають його в герметично закритому металевому корпусі, що поліпшує шумові, температурні та захисні властивості. У корпусі є спеціальне вікно, виготовлене з ІЧ-прозорого матеріалу, яке захищає чутливий елемент від зовнішніх впливів. На пластині,

розташованій всередині корпусу, знаходяться два збалансованих сенсора. Зона чутливості детектора PIR може мати різні форми, залежно від конструкції датчика.

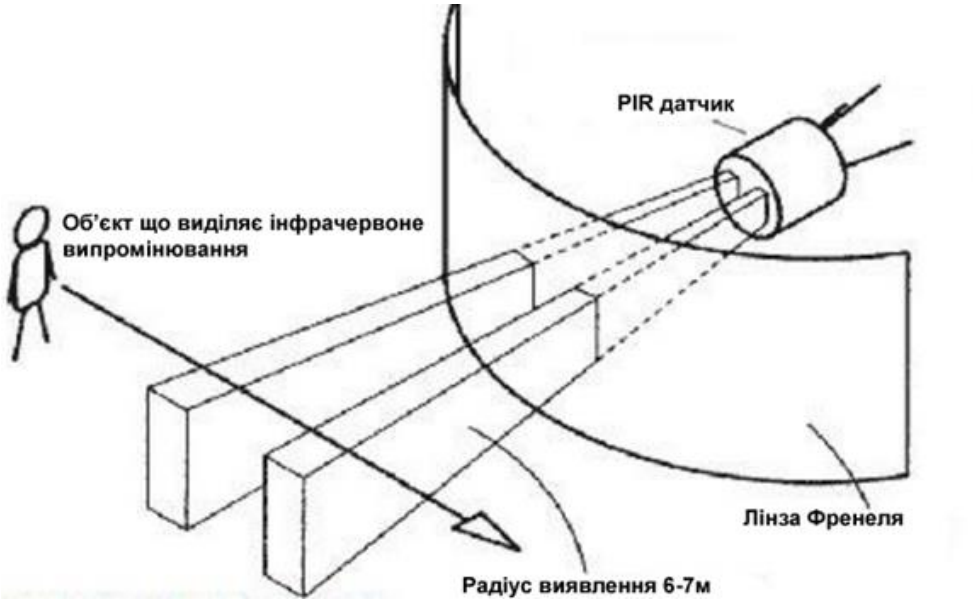


Рис. 1.4(ілюстрація роботи PIR датчика)

На відміну від інфрачервоних оптичних датчиків, які використовують LED - передатчик і ІЧ - приймач, PIR-сенсор нічого не випромінюванює, він працює в пасивному режимі, приймає слабке інфрачервоне випромінювання від об'єктів. Найбільш поширеним джерелом сигналу для сенсора PIR є організм людини, тому ця властивість успішно застосовується для автоматичного включення освітлення, системи сигналізації та відкривання дверей. Будь-який об'єкт, при температурі вище абсолютного нуля, є джерелом інфрачервоного випромінювання. Це невидиме випромінювання для очей людини, але не для піроелектричних матеріалів, які використовують PIR-датчик. При дії інфрачервоного випромінювання в піроелектричних матеріалах утворюється слабкий електричний заряд, схожий на заряд, що створюється в сонячних батареях. Температура тіла приблизно 34 градуса, як правило, вона вище, ніж температура загального фону. При знаходжені людини в зоні датчика, його більш висока температура викликає появу потенціалу в піроелектричному матеріалі. Електронною схемою посилюється

слабкий сигнал, створений інфрачервоним вилученням і далі подається на вхід диференціального компаратора. Компаратор зрівнює рівень сигналу з попередніми значеннями, що викликає його обробку. Насправді, це занадто простий механізм роботи, який може бути використаний з будь-яким джерелом випромінювання, у тому числі яскраве сонячне світло та відбиття від об'єктів у жаркі та сонячні дні.

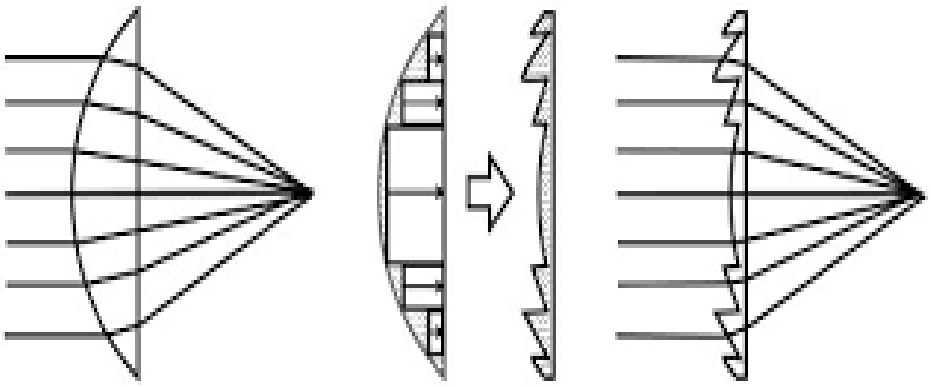


Рис. 1.5(ілюстрація роботи лінзи Френеля)

Лінза Френеля - це вид лінзи, що складається з ряду концентричних кілець або секторів, які виглядають як ламелі зубчастої корони. Вона отримала свою назву на честь французького інженера Огюстена Жана Френеля, який розробив її для оптичних систем у фарбах та фрезерних машинах.

Лінзи Френеля мають плоску форму та вони зазвичай виготовляються з пластику або акрилу. Вони мають меншу масу та товщину порівняно з традиційними скляними лінзами, що робить їх більш зручними для використання.

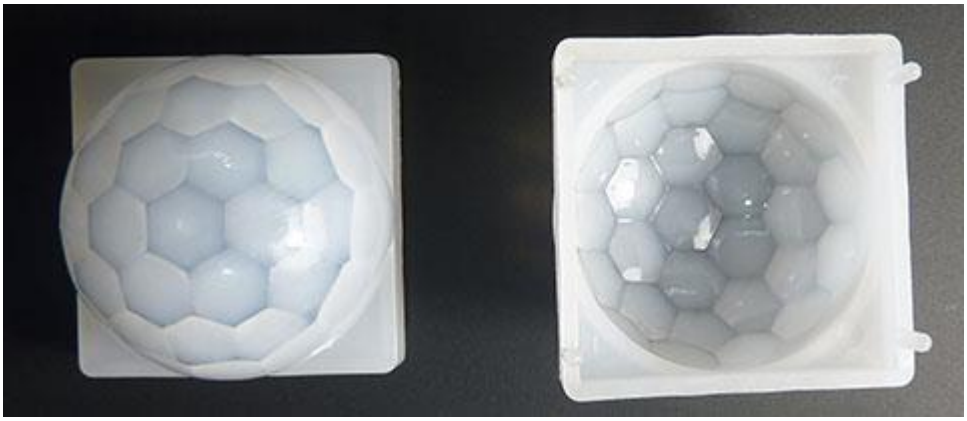


Рис. 1.6(лінза Френеля для PIR датчика)

У PIR датчику лінза Френеля використовується для покращення збору і фокусування інфрачервоних (теплових) променів, що випромінюються об'єктами. Лінза Френеля встановлюється перед датчиком і служить засобом що збільшує кут в якому датчик може зафіксувати рух.

1.5 Ультразвукові датчики руху

Ультразвуковий датчик руху працює на основі принципу звукової локації. Цей датчик складається з випромінювача, який генерує звукові хвилі, і мікрофона, який реєструє відбиті звукові хвилі. Випромінювач створює коливання з частотою від 25 до 40 кілогерц, а звукові хвилі, які відбиваються від перешкод, повертаються до джерела зміненою частотою через ефект Доплера.

Рис. 1.7(УЗ датчик)

Коли об'єкт рухається, звукові хвилі, що відбиваються від нього, змінюють свою частоту порівняно зі стартовою частотою, що була згенерована. Ці звукові коливання не сприймаються людським вухом, однак тварини, такі як собаки, відчувають їх і можуть бути чутливими до цих частот. Такі датчики можуть викликати дискомфорт у тварин і виникати проблеми в зв'язку з цим.

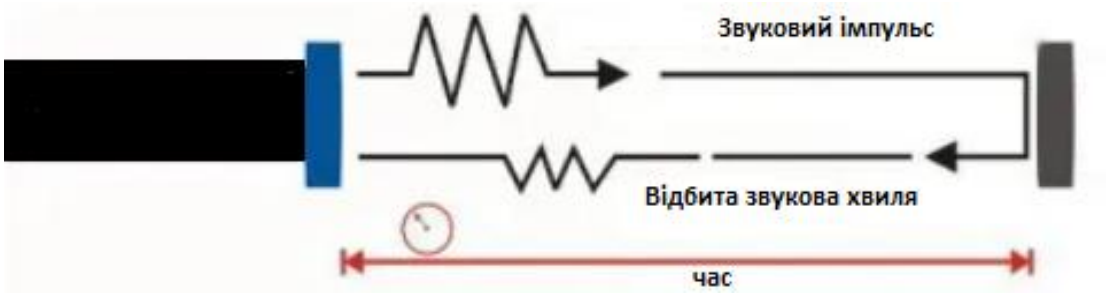


Рис. 1.8(ілюстрація роботи УЗ датчика)

1.6 Мікрохвильовий датчик руху

Ця технологія працює аналогічно до ультразвуку, але замість нього використовується випромінювання НВЧ (надвисокочастотні хвилі). Мікрохвильовий датчик руху здатний реагувати на рух об'єктів, що повністю або частково відбивають радіохвилі. Це можуть бути люди, тварини, металеві предмети та інші. Важливо, що датчик спроможний виявляти рух навіть за перешкодами, такими як дерева, двері, стіни з гіпсу, бетону, пластику, скла і таке подібне.

Рис. 1.9(МХ датчик)

Робота цього датчика ґрунтується на ефекті Доплера, який виявляється у зміні частоти відбитої хвилі через рух випромінювача, приймача або об'єкта, що відбиває хвилю. В даному модулі, частота радіохвилі, яку випромінює модуль, змінюється через рух об'єкта (перешкоди), що відбиває хвилю. Цей модуль складається з чипу, що має передавач та приймач. Датчик спрацьовує, коли приймач отримує сигнал, частота якого відрізняється від частоти сигналу, який висилає передавач.

Рис. 1.10(ілюстрація роботи МХ датчика)

Передавач випромінює радіохвилю на певній частоті. Якщо в зоні дії датчика немає об'єктів здатних відбивати радіохвилі, то приймач нічого не прийме й датчик не спрацює. Якщо в зоні дії датчика є нерухомі об'єкти здатні відбивати радіохвилі, то приймач прийме радіохвилю передавача, відбиту від цих об'єктів, але частота прийнятої радіохвилі буде дорівнює частоті сигналу передавача й датчик не спрацює. Якщо в зоні дії датчика є об'єкт здатний відбивати радіохвилі, який наближається до датчика (рухається), то приймач прийме відбиту від об'єкта радіохвилю, частота якої буде вище ніж в сигналу передавача й датчик спрацює. Якщо в зоні дії датчика є об'єкт здатний відбивати радіохвилі, який віддаляється від датчика (рухається), то приймач прийме відбиту від об'єкта радіохвилю, частота якої буде нижче ніж в сигналу передавача й датчик спрацює.

Використання цього датчика дозволяє виявляти рух навіть через об'єкти, які не відбивають радіохвилі, такі як кущі, трава, дерева, пластик, гіпс і т.д. Це робить його зручним для застосування на відкритих місцевостях. Проте, важливо враховувати, що якщо пристрої з однаковою частотою розташовані надто близько один до одного, вони можуть створювати взаємні перешкоди.

1.7 Комбіновані датчики руху

Вищеперераховані типи датчиків мають свої недоліки, через які ті чи інші датчики можуть спрацьовувати без необхідності, або не спрацьовувати коли така необхідність є. Інфрачервоні пасивні оповіщувачи можуть реагувати на радіатори, теплу підлогу і сонячні промені. Ультразвукові детектори не реагують на яскраве світло і температурні коливання, але не спрацюють якщо об'єкт рухається надто повільно. До того ж «бачать» через перешкоди, а УЗ-хвилі можуть викликати занепокоєння у тварин. В свою чергу НВЧ-датчики мають дальність дії кілька десятків, а іноді й сотень метрів та стійкі до засвічення і теплових потоків. Проте можуть реагувати на рухомі об'єкти за стінами приміщення, що охороняється та є шкідливим для людей і тварин.

Для цього існують комбіновані датчики руху. Вони спеціально створені і скомпоновані так, щоб перекривати недоліки один одного. І подають сигнал на централь лише тоді, коли активуються обидва датчики.

1.8 Датчики розбиття скла

Також в приміщеннях де є вікна, або в місцях де щось цінне лежить на вітрині має сенс задуматись про додатковий захист, а саме детектори розбиття скла. Детектори розбиття скла бувають різних типів від найстаріших до новіших варіантів.

1. Електроконтакта сповіщувач. Провід або фольгована смужка з діелектричним покриттям. По ньому йде струм. Це датчик удару: він забезпечує

механічний контроль, спрацьовує при спробі вирізати отвір або розбити матеріал (вдарити по ньому). Технологія застаріла і не експлуатується з причин, вказаних на початку статті.

2. П'єзоелектричний датчик розбиття, що реагує на механічні дії. Вловлює хвилі, що виникають при ударі. Відрізняють два типи: перша категорія вловлює інерційні імпульси і відразу ж спрацьовує. Друга - ловить коливання матеріалу до порушення його цілісності. Пристрої монтують на поверхні матеріалу. Серед недоліків - застосування тільки на невеликих площах, мала кількість налаштувань чутливості.

3. Акустичний датчик розбиття скла. Вловлює шуми, характерні для руйнування матеріалу. Як тільки виникають коливання в відповідному спектрі, відбувається спрацьовування.

Останній тип - найбільш сучасний і ефективний. Пристрої високочутливі, з великим діапазоном налаштувань. Вони розпізнають конкретні звуки, в залежності від типу матеріалу: наприклад, звук пошкодженого триплексного скла. Їх просто монтувати і підключати поруч з вікнами або вітринами, а не безпосередньо на них.

Принцип роботи сучасних датчиків розбиття скла базується на схемі фазо-частотного поділу, яка на порядок знижує кількість хибних тривог. Така технологія ґрунтується на прослуховуванні двох певних діапазонів частот. Сповіщувач піднімає тривогу лише в тому випадку, якщо спочатку фіксується інфранизкий звук від удару, а потім уже брязкіт розбитого скла.

Чутливість обох частотних каналів регулюється окремо, що дозволяє дуже тонко налаштувати прилад під параметри навколишнього середовища. Для перевірки правильності роботи використовуються спеціальні імітатори звуків.

1.9 Централь

Всі датчики що встановлені в приміщені самі по собі малоефективні в питаннях протидії проникненню на об’єкт так як не здатні самостійно відреагувати на акт проникнення. Для цього і існує централь або центральний блок керування. Принцип роботи центральної системи охорони будинку полягає в зборі і обробці інформації, яка надходить з різних датчиків, і відповідній реакції на будь-які виявлені загрози.

Коли будь-який з датчиків виявляє підозрілу активність, він надсилає сигнал до центральної системи охорони. Ця система аналізує отримані дані і приймає відповідні рішення. Наприклад, якщо система виявляє, що двері або вікно були відкриті, вона може сповістити власника про те, що потрібно перевірити стан приміщення. Або якщо датчик виявляє підозрілу активність в приміщенні, система може сповістити власника і, при необхідності, відправити попередження до служби безпеки або поліції.

1.10 Спрацьовування централі

Процес спрацьовування сигналізації в системі охорони будинку зазвичай складається з кількох етапів. Першим етапом є виявлення події, яка може спричинити спрацювання сигналізації. Це може бути рух в зоні захисту датчика, відкриття дверей або вікон, проникнення в приміщення, порушення інших параметрів, які були налаштовані в системі.

Після виявлення події система охорони проводить аналіз цієї події. Зазвичай цей аналіз здійснюється в центральному блоку системи, який отримує сигнали від всіх датчиків та інших компонентів системи. Якщо аналіз показує, що подія може бути пов'язана з порушенням безпеки, то система спрацьовує.

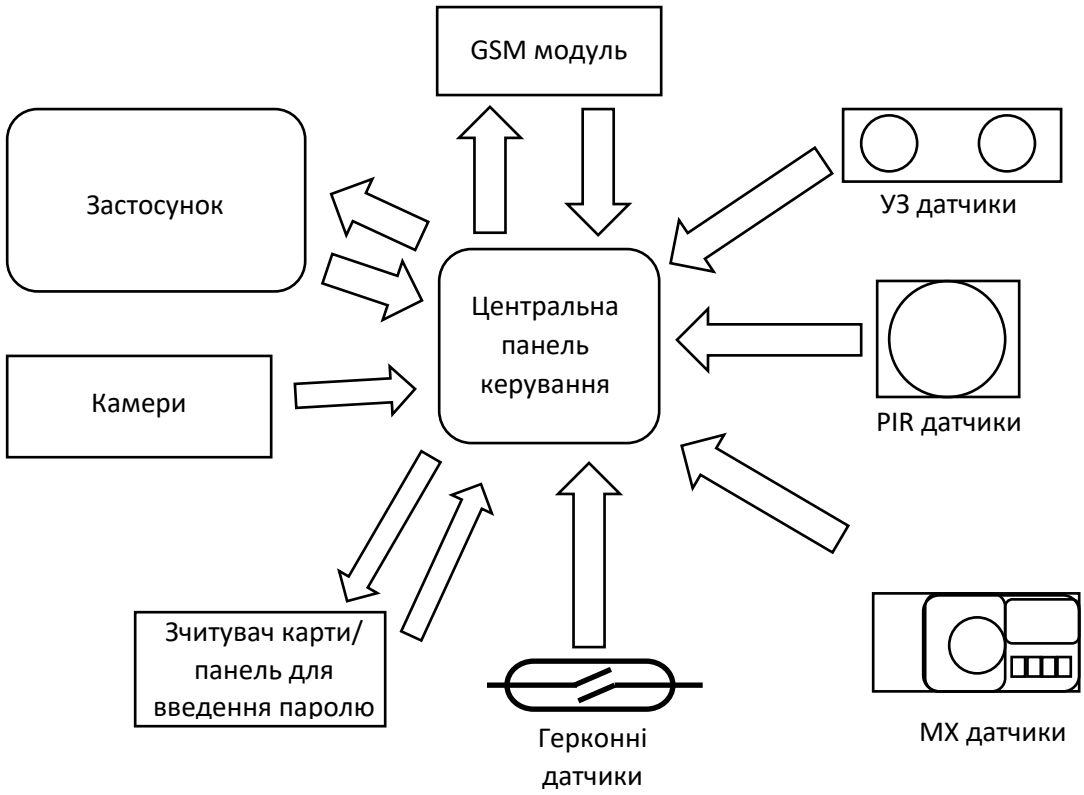


Рис. 1.11(Принципова схема взаємодії елементів системи сигналізації)

Спрацювання сигналізації може бути різного типу. Наприклад, система може виконати гучний звуковий сигнал або відправити повідомлення на мобільний телефон власника будинку. Деякі системи охорони можуть також відправляти повідомлення на пульт охорони, що дозволяє операторам з'єднатися з власником будинку та з'ясувати, що відбувається.

У деяких системах охорони також передбачені додаткові етапи. Наприклад, система може спочатку надіслати повідомлення на мобільний телефон власника будинку і попросити його ввести пароль для підтвердження, що він знає про подію. Якщо власник введе правильний пароль, то система може зупинити спрацьовування сигналізації. Якщо ж власник не введе правильний пароль або не підтвердить, що він знає про подію, то система продовжить опрацьовувати процедуру сигналізації, а також може надіслати повідомлення на пульт охорони для подальшої обробки.

Окрім цього, у деяких системах охорони передбачені додаткові функції, які можуть спрацювати під час спрацювання сигналізації. Наприклад, система може ввімкнути відеокамеру для запису відео з місця події, або активувати освітлення в зоні захисту, щоб запобігти можливому нападу. Деякі системи охорони також можуть відправляти повідомлення на сторонні сервіси охорони або на віддалений сервер, щоб забезпечити додатковий захист приміщення.

1.11 GSM модуль

GSM модуль (Global System for Mobile Communications) - це електронний пристрій, що використовується для передачі голосу та даних через мережу мобільного зв'язку. В системах сигналізації GSM модулі використовуються для забезпечення зв'язку між сигналізаційною панеллю та власником системи через мобільний зв'язок.

Принцип роботи GSM модулю базується на використанні SIM-карти (Subscriber Identity Module), яка містить інформацію про номер телефону та мережу оператора зв'язку. Модуль підключається до централі та має вбудовану антену для передачі та отримання сигналів.

Рис. 1.12(GSM модуль)

Коли центральна панель спостерігає будь-які небажані події, такі як вторгнення або спрацювання датчиків, вона активує GSM модуль. Модуль

встановлює зв'язок з оператором мобільного зв'язку, використовуючи SIM-карту, та передає інформацію про стан системи сигналізації.

GSM модуль може відправляти повідомлення SMS або набирати номера телефону, щоб повідомити власника про стан системи сигналізації. Повідомлення можуть містити інформацію про тип спрацьованого датчика або інше важливе повідомлення. Крім того, деякі GSM модулі підтримують передачу даних GPRS (General Packet Radio Service), що дозволяє використовувати Інтернет для передачі додаткової інформації.

Власник системи сигналізації може також взаємодіяти з системою через GSM модуль, надсилаючи SMS-команди для включення або виключення системи, перевірки стану або налаштування деяких параметрів.

1.12 RFID зчитувач

RFID (Radio Frequency Identification) зчитувач - це пристрій, який використовує радіочастотну технологію для безконтактного зчитування і запису даних на RFID-мітки або картки. В системах сигналізації RFID зчитувачі використовуються для контролю доступу та ідентифікації об'єктів.

Рис. 1.13(RFID зчитувач)

Принцип роботи RFID зчитувача полягає в наступних кроках:

- Зчитування: Зчитувач відправляє радіосигнал на певній частоті, що активізує RFID-мітку або картку, що знаходиться у зоні дії зчитувача.
- Взаємодія: Активована RFID-мітка чи картка відповідає на радіосигнал зчитувача, передаючи свою унікальну ідентифікаційну інформацію назад до зчитувача.
- Зчитування інформації: Зчитувач отримує передані дані від RFID-мітки або картки та інтерпретує їх. Ця інформація може містити унікальний ідентифікатор, тип об'єкта, додаткові дані або команди.
- Обробка даних: Зчитувач передає отримані дані до системи сигналізації для подальшої обробки. Система може використовувати ці дані для перевірки доступу, ідентифікації користувача або спрацювання певних сценаріїв в залежності від програмного забезпечення та конфігурації системи.

В системах сигналізації RFID зчитувачі можуть бути використані для контролю доступу до приміщень, активування або деактивування системи сигналізації при проходженні об'єктів через визначену зону, ідентифікації власника системи для включення або виключення сигналізації.

1.13 ВИСНОВКИ РОЗДІЛУ

Під час роботи над 1 розділом я проаналізував наявні на ринку рішення для систем контролю доступу до примішень. Використовуємі для цього датчики, плати та дотаткові елементи для зчитування RFID карток та GSM модуль. Також дослідив механізми взаємодії всих вищеперерахованих модулів.

РОЗДІЛ 2
РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕНЬ

2.1 Підбір плати(централі)

Основа всієї системи охорони це завжди центральний блок керування. Для своєї робот я обрав плату Arduino Uno, так як вона має в собі все необхідне для організації взаємодії всіх необхідних датчиків і панелі управління.

Arduino Uno - це відкрита платформа для розробки прототипів електронних проектів. Вона базується на мікроконтролері ATmega328P, який забезпечує можливість програмування і контролю різноманітних електронних пристроїв. Arduino Uno є однією з найпоширеніших і доступних моделей в лінійці Arduino.

Arduino Uno має вбудований мікроконтролер, а також набір цифрових і аналогових входів-виходів, які дозволяють підключати різноманітні датчики, актуатори і периферійні пристрої. Загалом, Arduino Uno є потужним інструментом для розробки і реалізації електронних проектів різного рівня складності і саме через це я обрав його як основу для своєї роботи.

Рис. 2.1 (плата Arduino Uno)

Вона має 32 кБ флеш-пам'яті, з яких 0.5 кБ використовується для зберігання завантажувального бутлоадера. Додатково, плата має 2 кБ оперативної пам'яті (SRAM) і 1 кБ EEPROM для зберігання постійних даних.

Цифрові входи/виходи: Arduino Uno має 14 цифрових входів/виходів (з яких 6 можуть бути використані як шим-виходи) для підключення до зовнішніх пристроїв та сенсорів. Кожен з цих входів/виходів може працювати з напругою 5 вольт.

Вона має 6 аналогових входів, які можуть приймати значення від 0 до 5 вольт. Кожен з цих входів має 10-бітний аналого-цифровий перетворювач (АЦП), що дозволяє зчитувати аналогові сигнали.

Arduino Uno має USB-порт для підключення до комп'ютера або іншого пристрою для програмування та зв'язку. Вона також має ICSP-роз'єм для програмування мікроконтролера за допомогою зовнішнього програматора. Крім того, плата має UART (серійний порт) і I2C (TWI) для зв'язку з іншими пристроями.

Arduino Uno може бути живлена з зовнішнього джерела напруги від 7 до 12 вольт або від USB-порту комп'ютера. Вбудований регулятор напруги забезпечує стабільне живлення мікроконтролера та підключених пристроїв. Номінальна робоча напруга для Arduino Uno становить 5 вольт.

Arduino Uno підтримує два апаратні переривання (interrupts), які можуть бути налаштовані для реагування на зміни сигналу на введених цифрових входах. Це дозволяє пристрою реагувати на зовнішні події в реальному часі.

Arduino Uno має компактний розмір, її розміри становлять близько 68.6 мм × 53.4 мм. Вона має невеликі розміри, що дозволяє мінімізувати розміри приладів на її основі.

Arduino Uno можна програмувати за допомогою мови Arduino, яка базується на мові C/C++. Існує ряд середовищ для розробки (наприклад, Arduino IDE), які надають зручний інтерфейс для розробки програм для Arduino.

Вищеперераховані характеристики плати повністю відповідають всім вимогам до основи автоматизованої системи контролю доступу до приміщень. Її компактність, універсальність і кількість розмірів є основними факторами для вибору саме її у якості централі.

2.2 Підбір датчиків

Враховуючи специфіку виробничих приміщень, а саме шляхи можливого потрапляння всередину та специфіку використання приміщення, для проектування системи контролю доступу, я обрав наступні види датчиків.

Герконні датчики підходять для систем сигналізації через свою простоту використання, надійність, виявлення відкриття/закриття і широкий діапазон застосувань. Вони легкі у встановленні, не мають складних налаштувань, мають малу кількість рухомих частин, точно виявляють стан відкриття/закриття і можуть використовуватись в різних системах сигналізації для виявлення недопустимого доступу або руху.

Вони мають бути встановлені на всіх можливих дверях, вікнах, та люках через які можна потрапити до приміщення. Сам геркон встановлюється на раму дверей чи вікон за відкриттям яких він буде слідкувати в безпосередній близькості від нього встановлюється магніт. Сам магніт встановлюється на двері чи вікно так щоб в закритому стані магніт активував геркон. Так як показано на рисунку:

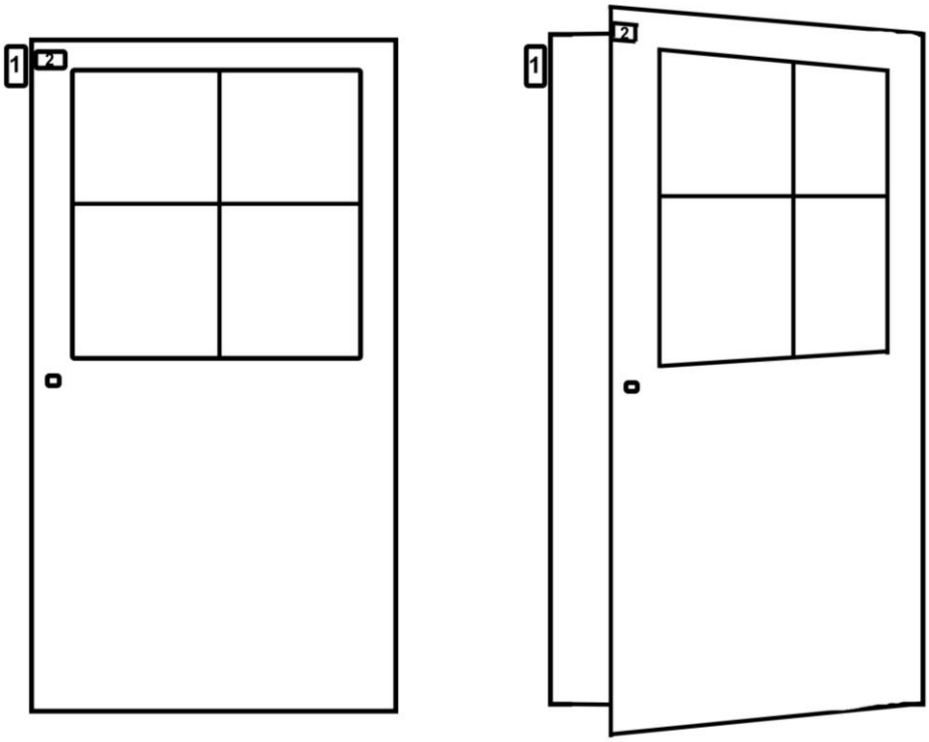


Рис. 2.2 (1- геркон встановлений на рамі дверей, 2- магніт встановлений на дверях)

Відповідно для кожного геркона в системі має бути така або подібна схема підключення до плати Arduino:

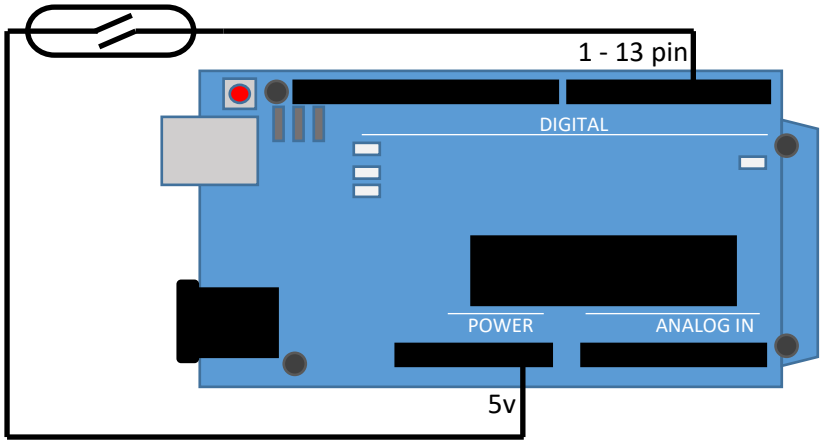


Рис. 2.3(схема підключення геркону)

Для даного проекту я обрав геркон що замикає ланцюг живлення при наближенні магніту, що певним чином по впливає на код програми. В такому випадку система повинна буде реагувати саме на розмикання ланцюга живлення

Інфрачервоні датчики руху теж мають бути розміщені в можливих місцях проникнення являючи собою додатковий захист таких вузлів. Для цієї роботи я обрав датчик HC-SR501. HC-SR501 є популярним PIR (пасивним інфрачервоним) датчиком руху, який використовується в багатьох проектах автоматизації та сигналізації. Підключення PIR датчику до плати Arduino здійснюється за наступною схемою:

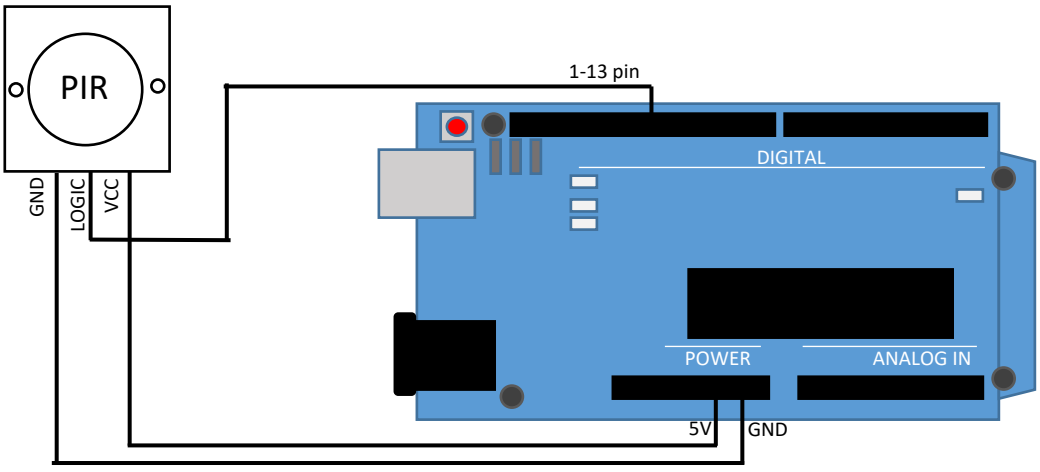


Рис. 2.4(схема підключення PIR датчику)

Датчик працює з робочою напругою в діапазоні 4,5-20 В. HC-SR501 має налаштовувану чутливість, яка дозволяє регулювати його реакцію на рух об'єктів. Чутливість може бути налаштована за допомогою потенціометра, що дозволяє пристосувати датчик до різних сценаріїв застосування.

Датчик має широкий кут охоплення, який становить приблизно 120 градусів та може виявляти рух на відстані до 7 метрів. Це робить його придатним для використання в середніх і великих приміщеннях.

Коли датчик виявляє рух, він видає цифровий вихідний сигнал на виході. Зазвичай використовується вихідний сигнал на рівні логічної "1", який змінюється на "0" після вимкнення датчика. Це помітно спрощує роботу з даним датчиком і робить його сумісним з обраною вище платою.

Враховуючи особливості цієї моделі і принцип її роботи встановлювати його необхідно біля місць потенційного проникнення(ними можуть бути входи, в'їзди до приміщення та вікна) так, щоб потрапляючи до будівлі радіус дії датчику неможливо було уникнути.

2.3 Підбір решти складових

Для вмикання і вимкнення системи сигналізації я використав **RFID зчитувач** та ключ картку. Встановлений зчитувач має бути з зовнішньої сторони будівлі окремо від плати ARDUINO, її краще встановити всередину будівлі це ускладнить взлом ситеми. Модель зчитувача RC 522 має наступну схему підключення:

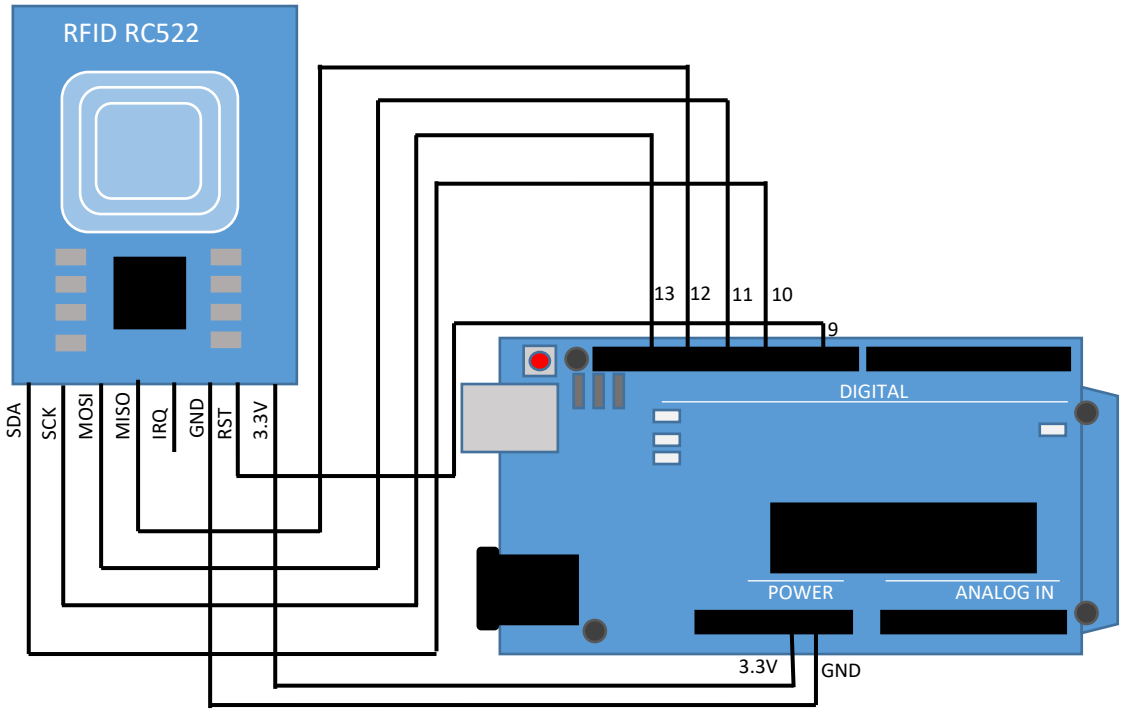


Рис. 2.5(схема підключення RFID зчитувача)

Також для **сигналізування про проникнення** на об’єкт системі необхідний динамік. Для цієї задачі був обраний TMB12A05, який має наступну схему підключення.

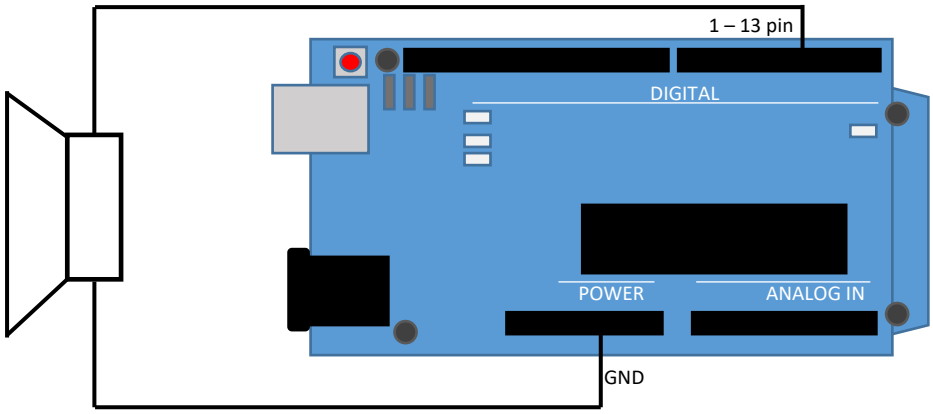


Рис. 2.6(схема підключення динаміку)

Але динамік своїм шумом в кращому випадку налякає зловмисника, але не прийме ніяких запобіжних дій. Для вирішення цієї проблеми можна проінформувати власника, який в свою чергу прийме рішення про подальші дії. Для цього в систему сигналізації буде встановлений SIM800L. До плати він буде підключатись наступним чином:

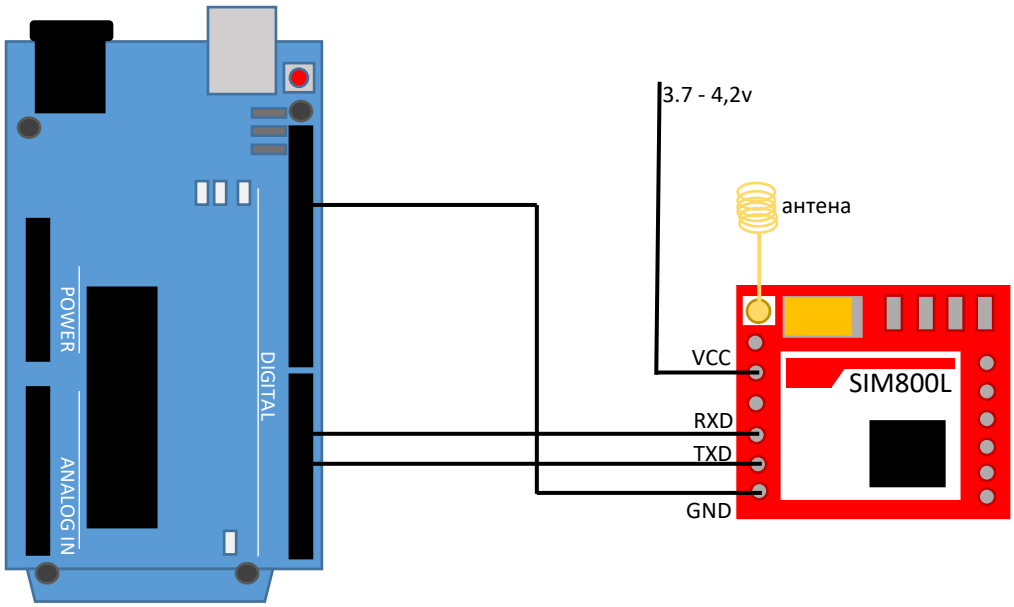


Рис. 2.7(схема підключення GSM модуля)

2.4 ЗАГАЛЬНА СХЕМА

Загальна схема системи контролю доступу до виробничих приміщень виглядає наступним чином:

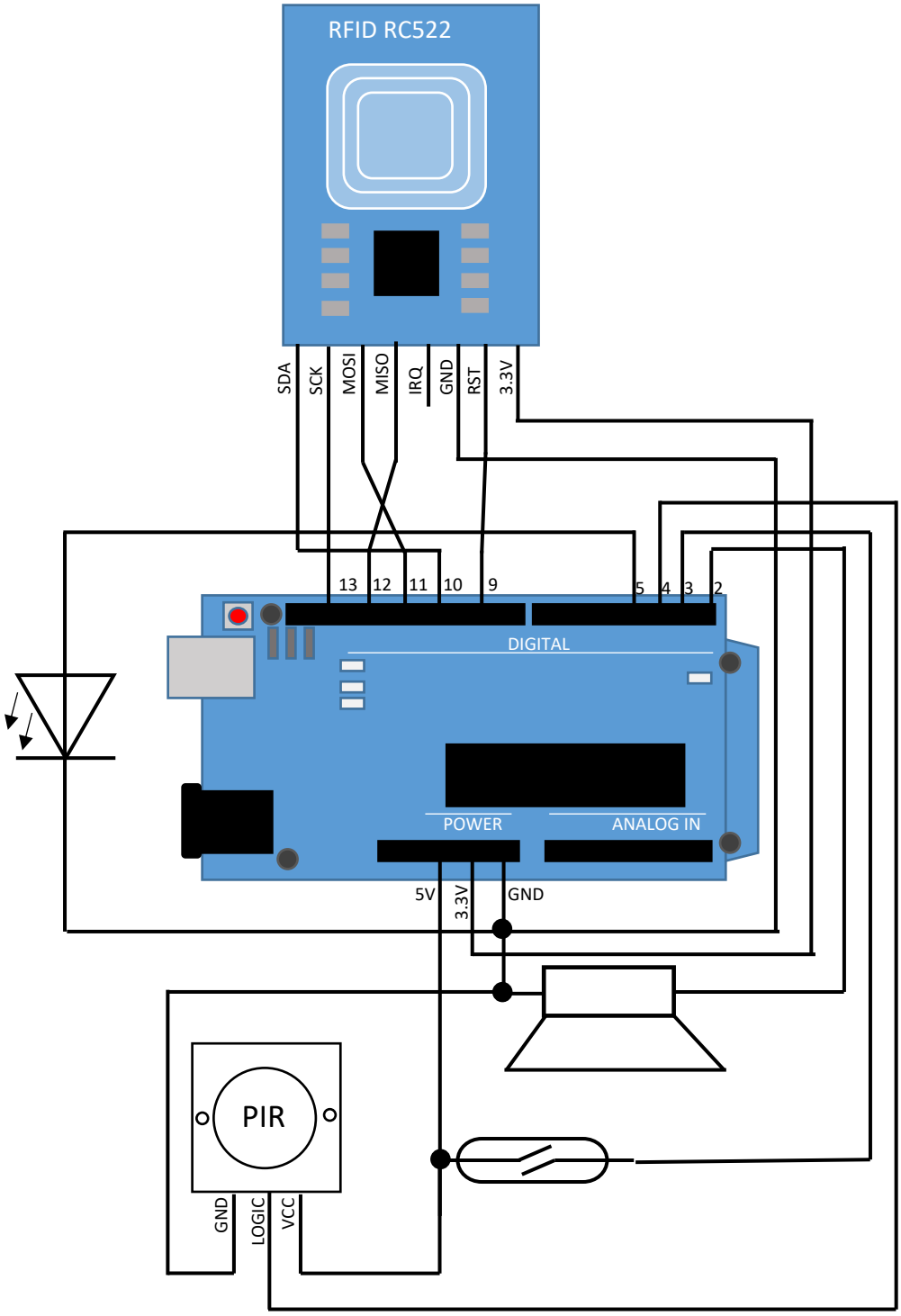


Рис 2.8 (загальна схема сигналізації)

На схемі зображена схема з одним PIR датчиком та одним герконом, але за потреби можна збільшити їх кількість до необхідної підключивши подібним чином.

2.5 ВИСНОВКИ РОЗДІЛУ

Під час роботи над цим розділом я обрав комплектуючі для системи автоматичного контролю доступу до виробничих приміщень. Дослідив методи їх підключення до центральної плати і розробив загальну схему сигналізації.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ФУНКЦІОНУВАННЯ СИСТЕМИ

Основна ідея даної системи помітити і відреагувати на несанкціоноване проникнення на об’єкт. Для цього система буде мати 2 режими закритий і відкритий. Перемикання між режимами відбувається за допомогою RFID зчитувача. При притулянні картки до зчитувача алгоритм зчитує унікальний номер картки і звіряє його з номерами що записані в код програми і якщо номер співпадає режими перемикаються в противному випадку ні. Індикатором режимів є діод на 5-ому піні, якщо він горить система в закритому режимі, якщо ні то у відкритому.

При відкритому режимі сигналізація не спрацює ні від якого датчику. Якщо ж ввімкнений закритий режим то при спрацьовуванні датчиків подається сигнал на динамік і вмикається сигналізація. Вимкнути сигналізацію можна притуливши картку. Якщо UID код притуленої картки не співпадає з заданим то діод що відображає режим роботи блимне один раз. Це зроблено для того щоб було видно що зчитування картки відбулося.

3.1 Опис коду

З самого початку коду йдуть директиви #include що підключають до проекту 3 бібліотеки. “SPI.h” – бібліотека призначена для роботи з пристроями що підтримують SPI. “MFRC522.h” - бібліотека призначена для роботи зі зчитувачем карток RC522. “SoftwareSerial.h” - дозволяє реалізувати послідовний інтерфейс на будь-яких цифрових виходах Ардуїно за допомогою програмних засобів, що дублюють функціональність UART (звідси і назва SoftwareSerial). Бібліотека дозволяє програмно створювати кілька послідовних портів, що працюють на швидкості до 115 200 бод. Для пристроїв, що працюють з інвертованим сигналом, у бібліотеці передбачено відповідний параметр, що включає інвертування.

```
#include <SPI.h>
#include <MFRC522.h>
#include <SoftwareSerial.h>
```

Вводимо змінну для стану сигналізації, 0 - сигналізація відкрита, 1 - сигналізація закрита.

```
bool state = 0;  // змінна що відповідає за стан сигналізації 0 - відкр; 1 - закр;
```

Далі створюємо об’єкт типу mfrc522 через який буде реалізована робота з відповідним модулем зчитування і визначаємо змінні для відповідних пінів SS і RST. А також об’єкт типу SoftwareSerial для роботи з модулем sim800l і також для нього визначаємо RX та TX піни.

```
#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);  // Створюємо об'єкт MFRC522
#define RX_PIN 7
#define TX_PIN 6
SoftwareSerial sim800l(RX_PIN, TX_PIN); // RX, TX піни для з'єднання з модулем SIM800L
```

Після цього нам треба задати змінні для пінів інших сенсорів і приладів.

```
int DiodePin = 5;  // записуємо піни для діода, PIR сенсора, геркона та динаміка
int PIRsensPin = 4;
int GERKsensPin = 3;
int DynamicPin = 2;
```

Далі нам треба задати змінні для UID картки яка буде відкривати та закривати систему та змінну для номеру на який будуть приходити повідомлення про стан системи.

```
char savedCardID[] = "13b44f0e";  // Зберігаємо унікальний номер пластикової картки
```

```
String number = "+380980001122"; // номер на який будуть надсилатись повідомлення
```

В функції setup() ми визначаємо швидкість передачі даних для модуля SIM800L, ініціалізуємо шину SPI та ініціалізуємо модуль RC522.

```
void setup() {
  sim800l.begin(9600); // Швидкість передачі даних для модуля SIM800L
  SPI.begin();         // Ініціалізуємо шину SPI
  mfrc522.PCD_Init();  // Ініціалізуємо модуль RC522
```

Також для плати Arduino важливо визначити варіант роботи(ввід\вивід) для кожного піну.

```
pinMode(DiodePin, OUTPUT);  // призначаємо піни для діода, PIR сенсора, геркона та динаміка
  pinMode(PIRsensPin, INPUT);
  pinMode(GERKsensPin, INPUT);
  pinMode(DynamicPin, OUTPUT);
```

Функцію loop() ми починаємо з оновлення стану діода це дуже важливо щоб він відображав актуальну інформацію про стан системи.

```
digitalWrite(DiodePin, state); // оновлюємо стан діода
```

Далі ми зчитуємо інформацію з усіх датчиків і відповідним чином її обробляємо. Якщо рух був помічений система відправляє смс повідомлення власнику і вмикає сирену.

```
  bool pirSens = digitalRead(PIRsensPin);  // зчитування PIR датчику
  bool gerkSens = digitalRead(GERKsensPin);   // зчитування Gerk датчику
  if((pirSens == 1 || gerkSens == 1) && state == 1) // спрацьовування PIR та Gerk датчиків
    {
```

```
    sendSMS(number, "Зафіксовано проникнення"); // Повідомляє по СМС про проникнення
    digitalWrite(DynamicPin, HIGH);  // вмикання сирени
  }
```

Після цього ми перевіряєм чи піднесена картка до зчитувача і якщо картка піднесена ми зчитуємо інформацію з картки.

```
if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) // Перевіряємо, чи є пластикова картка поблизу
 {
  // Отримуємо унікальний номер пластикової картки
  String cardID = "";
  for (byte i = 0; i < mfrc522.uid.size; i++)
  {
    cardID += String(mfrc522.uid.uidByte[i] < 0x10 ? "0" : "");
    cardID += String(mfrc522.uid.uidByte[i], HEX);
  }
```

Після зчитування ми звіряємо UID картки з заданим завчасно і якщо номери співпадають ми змінюємо стан системи. І якщо номер картки не співпадає діод стану системи блимне.

```
// Порівнюємо отриманий унікальний номер зі збереженим
  if (cardID.equals(savedCardID))
  {
    state == 0 ? state = 1 : state = 0; // змінюємо стан системи якщо картка підійшла

    sendSMS(number, state == 0 ? "Alarm off" : "Alarm on"); // Повідомляє по СМС стан сигналізації
```

```
    digitalWrite(DynamicPin, LOW); // скидуємо тривогу якщо вона активована
    pirSens = 0;
    gerkSens = 0;
  }
  else
  {
     if(state == 0)   // діод мигне якщо карта не підходить
     {
      digitalWrite(DiodePin, 1);
      delay(500);
      digitalWrite(DiodePin, 0);
     }
     else
     {
      digitalWrite(DiodePin, 0);
      delay(500);
      digitalWrite(DiodePin, 1);
     }
  }
```

Потім зупиняємо комунікацію з картою.

```
  mfrc522.PICC_HaltA();  // Зупиняємо комунікацію з карткою
```

В коді використовується функція sendSMS(). В ній описана вся необхідна комунікація з модулем SIM800L для відправки СМС повідомлення на переданий в параметрі телефон, також передане в параметрі повідомлення.

```
void sendSMS(String phoneNumber, String message) {
 sim800l.println("AT+CMGF=1"); // Встановлення режиму текстових повідомлень
 delay(1000);
```

```
  sim800l.println("AT+CMGS=\"" + phoneNumber + "\""); // Встановлення номеру отримувача
  delay(1000);

  sim800l.println(message); // Відправка повідомлення
  delay(1000);

  sim800l.println((char)26); // Код ASCII для Ctrl+Z
  delay(1000);

  Serial.println("SMS відправлено.");
}
```

3.2 Висновки розділу

Під час роботи над цим розділом я дослідив і обрав необхідні для вищеперерахованих елементів бібліотеки. А також написав код для взаємодії всіх елементів системи сигналізації та налагодив його коректне функціонування.

ВИСНОВКИ

В цій бакалаврській дипломній роботі проаналізовано попит на системи сигналізації, основні задачі сучасних систем сигналізації, методи та засоби за допомогою яких вони виконують покладене на них завдання. Були проаналізовані вже наявні на ринку комплексні рішення. Також були проаналізовані датчики що використовуються в подібних системах. Були розглянуті принципи роботи та порівняні сильні і слабкі сторони можливих датчиків. Було досліджено та описано механізм спрацьовування систем сигналізації. Додатково були досліджені і розібрані принципи роботи RFID зчитувача і його застосування в подібних системах. Також був вивчений принцип роботи GSM модуля та його функціоналу необхідного для оповіщення власника приміщення про потенційне проникнення.

Під час роботи над безпосередньо системою сигналізації було порівняно та обрано найбільш підходящі саме для виробничих приміщень датчики руху. А саме герконні та PIR датчики. Було обрано спеціальні пристрої та налагоджено їх роботу з оповіщення власника приміщень про можливе проникнення в виробничі приміщення. А також було організовано додаткові заходи безпеки доступу до керування системою контролю доступу до виробничих приміщень. А саме за допомогою RFID зчитувача та відповідної картки.

Для погодження роботи вузлів сигналізації одного з іншим був написаний, скомпільований та завантажений до мікроконтролера Arduino UNO відповідний код. Принцип роботи цієї програми був додатково описаний в блок схемі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Automated system for remote monitoring of the sprinkling machines status | AA Omelchuk, YO Lebedenko, OV Polyvoda - Прикладні питання математичного моделювання, 2019
2. What is a Reed Switch and How Does it Work? | (URL: https://www.arrow.com/en/research-and-events/articles/the-reed-switch-ingeniously-simple-sensing) (12.06.2023)
3. How PIRs Work | (URL: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/how-pirs-work) (12.06.2023)
4. How Ultrasonic Sensors Work | (URL: https://maxbotix.com/blogs/blog/how-ultrasonic-sensors-work) (12.06.2023)
5. GSM (Global System for Mobile communication) | (URL: https://www.techtarget.com/searchmobilecomputing/definition/GSM) (12.06.2023)
6. Геркон | (URL: https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D1%80%D0%BA%D0%BE%D0%BD) (13.06.2023)
7. Як працює датчик відкриття дверей: що таке геркон та який принцип його роботи | (URL: https://ohrana.ua/uk/stati-i-obzory/kak-rabotaet-datcik-otkrytiya-dveri-cto-takoe-gerkon-i-princip-ego-raboty.html) (13.06.2023)
8. PIR-датчик: все, що вам потрібно знати | (URL: https://www.hwlibre.com/uk/sensor-pir/) (13.06.2023)
9. PIR датчик руху Arduino HC-SR501 | (URL: https://wiki.tntu.edu.ua/PIR_%D0%B4%D0%B0%D1%82%D1%87%D0%B8%D0%BA_%D1%80%D1%83%D1%85%D1%83_Arduino_HC-SR501) (13.06.2023)
10. Датчик руху | (URL: https://corelamps.com/elektormontazhne-obladnannia/datchyk-rukhu/) (13.06.2023)

11. Системи контролю та управління доступом. Огляд. URL: https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review (дата звернення: 16.02.2023)
12. Системи охорони периметра URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/perimeter-security-systems (дата звернення: 16.02.2023)
13. Інструкція з використання Hub URL: https://support.ajax.systems/uk/manuals/hub/ (дата звернення: 16.02.2023)
14. Як працюють датчики руху URL: https://www.bezpeka-shop.com/ua/blog/obzor/kak-rabotayut-datchiki-dvizheniya/ (дата звернення: 16.02.2023)
15. Датчик руху URL://corelamps.com/elektormontazhne-obladnannia/datchyk-rukhu/ (дата звернення:16.02.2023)
16. Kondratieva, I.U. Using Entropy Estimation to Detect Moving Objects / I.U. Kondratieva , H.V. Rudakova , O.V. Polyvoda , Yu.O. Lebedenko, V.V. Polyvoda // 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial VehiclesDevelopments, APUAVD 2019 - Proceedings, pp. 270-273.
17. An Introduction to MEMS (Micro-electromechanical Systems) URL: https://www.lboro.ac.uk/microsites/mechman/research/ipm-ktn/pdf/Technology_review/an-introduction-to-mems.pdf (дата звернення: 16.02.2023)
18. Fire Alarm Systems | Smart / Wireless Systems – Kisi URL: https://www.getkisi.com/guides/fire-alarm (дата звернення: 16.02.2023)
19. Сучасні підходи оцінки якості характеристик складних електричних кіл / В. Б. Дроменко, В. С. Тарас. // Технології та дизайн. - 2021. - № 1. - Режим доступу: http://nbuv.gov.ua/UJRN/td_2021_1_10 (дата звернення: 16.06.2023)

20. Застосування мікросистеми збору даних з інтерфейсом USB m-DAQ12/DAC для автоматизації швидкоплинних технологічних процесів / Лісовець С.М., Дроменко В.Б., Кучма Р.А., Бондаренко С.В. // Інноватика в освіті, науці та бізнесі: виклики та можливості: Матеріали I Всеукраїнської конференції здобувачів вищої освіти і молодих учених (17 листопада 2020 р., м. Київ). – К. : КНУТД, 2020. – С. 278-285.
21. Моделювання автоматизованої системи оперативного управління параметрами "розумного будинку" в середовищі PROTEUS / А. М. Бойко, В. Б. Дроменко. // Технології та дизайн. - 2020. - № 2. - Режим доступу: http://nbuv.gov.ua/UJRN/td_2020_2_16 (дата звернення: 16.06.2023)
22. Дослідження датчиків руху для застосування у автоматизованій системі управління зовнішнім освітленням вулиць / В. Б. Дроменко, Т.О. Лавренюк, О.О. Кушнір // Вісник інженерної академії України / Теоретичний і науково-практичний журнал інженерної академії України. – К.: НАУ, 2019, № 4, – С. 189-192.
23. The Solar Lamp Works as Needed | (URL: https://projecthub.arduino.cc/cvzeljko/the-solar-lamp-works-as-needed-f6e4b3) (16.06.2023)
24. RFID NeoPixel access project | (URL: https://projecthub.arduino.cc/Werzaire/rfid-neopixel-access-project-37a293) (16.06.2023)
25. Arduino UNO | (URL: https://www.javatpoint.com/arduino-uno) (16.06.2023)
26. Мікропроцесорна платформа Arduino: конспект лекцій з дисципліни «Мікропроцесорні та програмні засоби автоматизації». Мікропроцесорна платформа Arduino для студентів освітнього рівня «Бакалавр» спеціальності – 151 Автоматизація та комп’ютерно-інтегровані технології. / упор. Ю. М. Пилипенко. – Київ. : КНУТД, 2023.

Додаток А

УДК 004.934:681.5

К.М. Вітер, Ю.О. Лебеденко, О.А. Гром'як
Київський національний університет технології та дизайну
kostyaviter@gmail.com

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО ВИРОБНИЧИХ ПРИМІЩЕНЬ

Питання захисту власного майна стояла перед людством ще з самого першого дня нашого існування. І рівно з тим як росли й вдосконалювались в своїх підходах до крадіжок злочинці, так і розвивались і ускладнювались методи захисту від них. І в наші часи це питання досі не втратило своєї актуальності. Тим паче в місцях де багато цінних речей. Одним з варіантів таких місць є виробничі приміщення, де сконцентровані як і дороговартісне обладнання, так і продукція, що виготовляється на ньому.

Вирішити цю проблему в наші часи призвані охоронні системи. Такі системи здатні без участі людей, або з мінімальним їх залученням контролювати хто потрапляє до приміщення, фіксує всі несанкціоновані спроби проникнення та вживає відповідних заходів [1].

Подібні системи, як правило, дуже унікальні бо проектуються окремо під кожен об'єкт та кожне приміщення. Але попри це складаються з подібних основних та допоміжних компонентів (рис. 1) [2].

До обов'язкових належать:

- Централь
- Прилади керування(можуть бути вбудовані в централь)
- Датчики руху/відкриття

До додаткових(не обов'язкових) відносяться:

- Пульти керування
- Мобільний застосунок
- Камери
- Датчики диму/вологи

Хоч кожна система і унікальна по своєму, але суть їх роботи однакова. Завжди є певна сукупність датчиків, котрі фіксують проникнення на об'єкт. Як правило їх розставляють в місцях потенційного проникнення, та біля найцінніших об'єктів. Це можуть бути вікна, двері, люки в'їзди, виїзди вентиляції та інші шляхи що ведуть до приміщення.

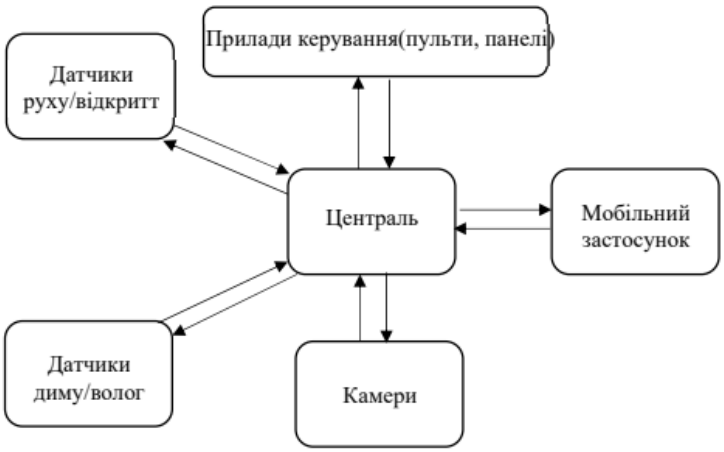


Рисунок 1 – Структура системи контролю доступу до виробничих приміщень

Помітивши проникнення, датчики подають сигнал на центральний блок керування (централь). Централь, в свою чергу, опрацьовує цей сигнал в залежності від запрограмованого сценарію та вбудованих в неї модулей. При спрацьовуванні блок керування може або просто увімкнути сигналізацію, або відправити на телефон власника повідомлення, або сповістити про проникнення відповідні служби. Встановлюється централь якомога глибше в центрі приміщення щоб ускладнити доступ до неї потенційних злочинців.

Також важливою частиною системи захисту є панель управління. Через неї власник приміщень отримує доступ до керування системою. Панель в свою чергу має бути встановлена біля основного входу в приміщення, в залежності від панелі власник приміщення отримує доступ до керування системою через ключ-карту, або пароль [3].

Для правильного функціонування системи необхідно правильно підібрати датчики щоб правильно перекрити ними можливі точки проникнення. Герконні датчики руху, вони ж датчики відкриття, встановлюються на двері чи вікна [4, 5]. Через свої особливості вони ідеально підходять саме під цю задачу. В випадку, коли треба покрити певну область, використовуються інші датчики руху: інфрачервоний, ультразвуковий чи мікрохвильовий, в залежності від площі, що треба покрити [6]. Також доцільно застосовувати інтегральні акселерометричні датчики, виконані за сучасною MEMS-технологією [7,8].

Більшість виробництв мають потребу не тільки в контролі доступу до приміщень, а і в системі протипожежного захисту [9]. І більшість компаній на ринку пропонують лише одне з необхідних рішень. Але набагато зручніше для фінального користувача було б додати систему виявлення, а можливо і гасіння пожежі безпосередньо в систему контролю доступу та об'єднати два інтерфейси керування в один.

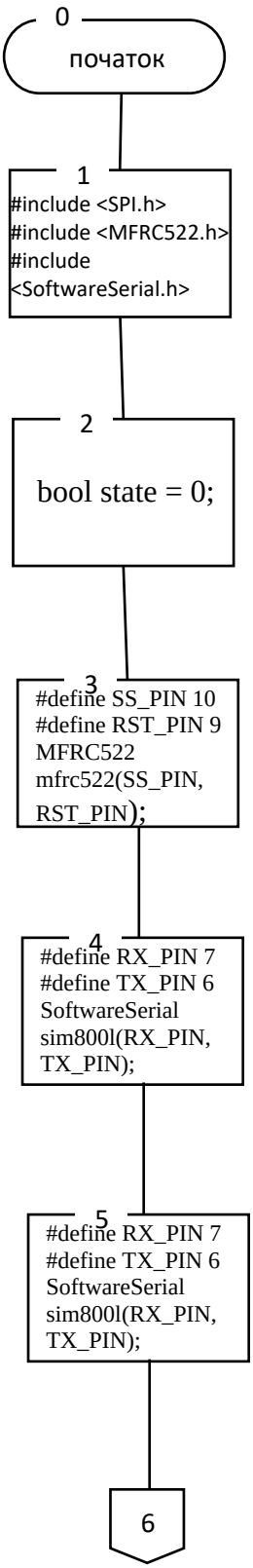
В сучасних системах існує можливість дистанційного керування системою, яке може бути організоване як через пульт дистанційного керування, так і через застосунок в телефоні, якщо пульт має обмеження і в дистанції роботи і в функціоналі. А забезпечивши централь доступом до інтернету можна організувати керування нею через застосунок в телефоні, а це значно розширює можливості керування системою. Використовуючи застосунок, можна показати власнику зображення з камер при спрацьовуванні датчиків. І надати власнику можливість обрати варіанти реагування на інцидент, що дозволяє запобігати хибним спрацьовуванням.

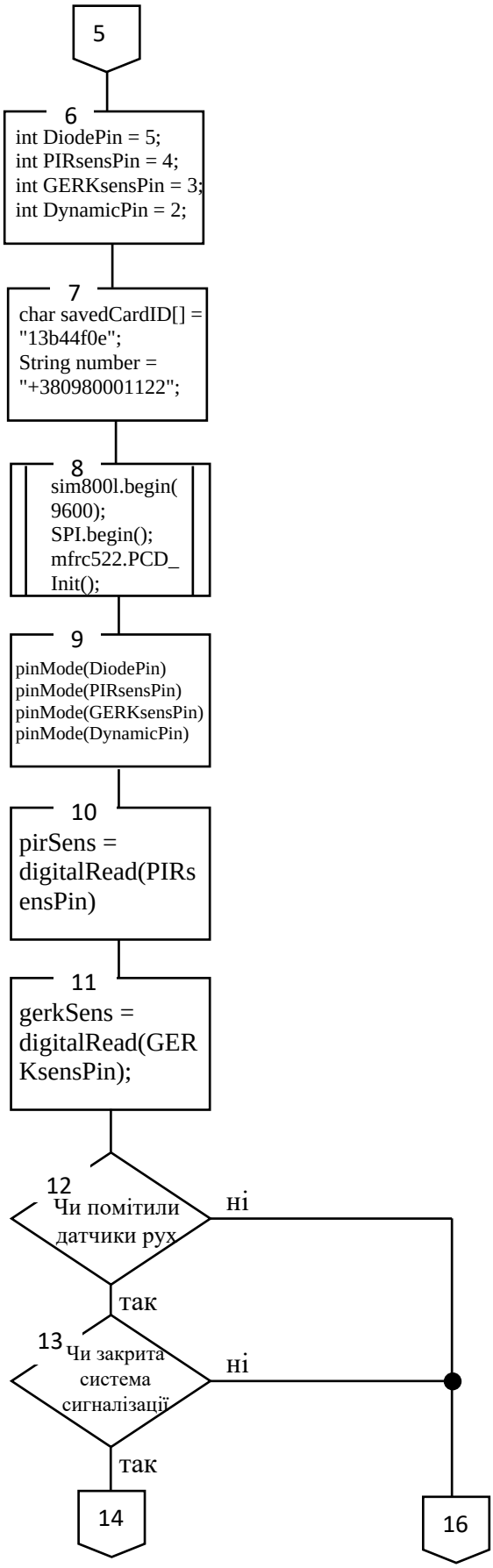
ЛІТЕРАТУРА:

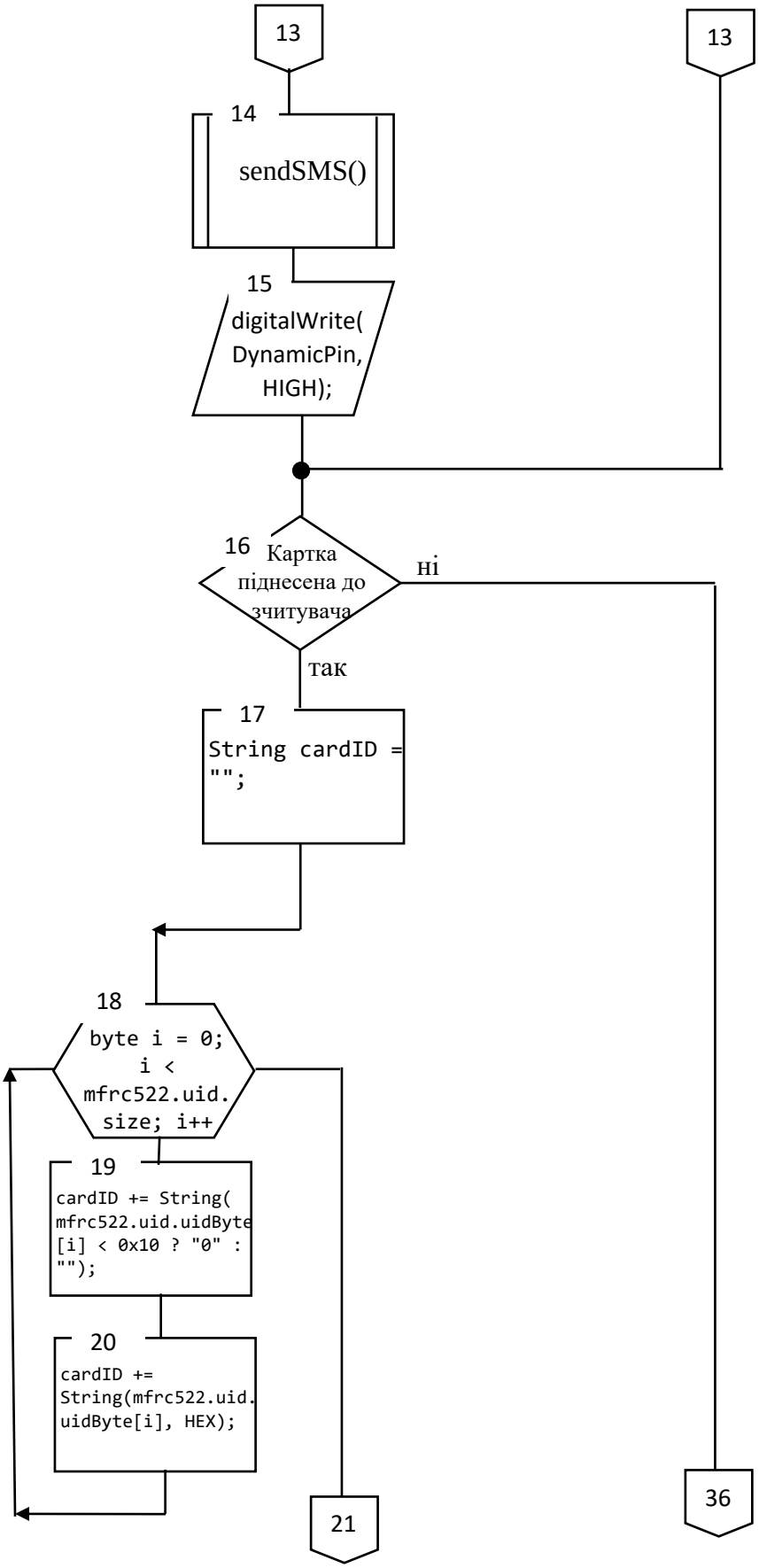
1. Системи контролю та управління доступом. Огляд. URL: https://valtek.com.ua/ua/system-integration/security-control-system/access-control/access-control-review (дата звернення: 16.02.2023)
2. Системи охорони периметра URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/perimeter-security-systems (дата звернення: 16.02.2023)
3. Інструкція з використання Hub URL: https://support.ajax.systems/uk/manuals/hub/ (дата звернення: 16.02.2023)
4. Як працюють датчики руху URL: https://www.bezpeka-shop.com/ua/blog/obzor/kak-rabotayut-datchiki-dvizheniya/ (дата звернення: 16.02.2023)
5. Датчик руху URL://corelamps.com/elektormontazhne-obladnannia/datchyk-rukhu/ (дата звернення: 16.02.2023)
6. Kondratieva, I.U. Using Entropy Estimation to Detect Moving Objects / I.U. Kondratieva , H.V. Rudakova , O.V. Polyvoda , Yu.O. Lebedenko, V.V. Polyvoda // 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial VehiclesDevelopments, APUAVD 2019 - Proceedings, pp. 270-273.
7. An Introduction to MEMS (Micro-electromechanical Systems) URL: https://www.lboro.ac.uk/microsites/mechman/research/ipm-ktn/pdf/Technology_review/an-introduction-to-mems.pdf (дата звернення: 16.02.2023)
8. Омельчук А.А., Лебеденко Ю.О., Поливода О.В. Автоматизована система віддаленого моніторінгу стану дощувальних машин. *Прикладні питання математичного моделювання*, 2019 №1, т 2, С. 89-97.
9. Fire Alarm Systems | Smart / Wireless Systems – Kisi URL: https://www.getkisi.com/guides/fire-alarm (дата звернення: 16.02.2023)

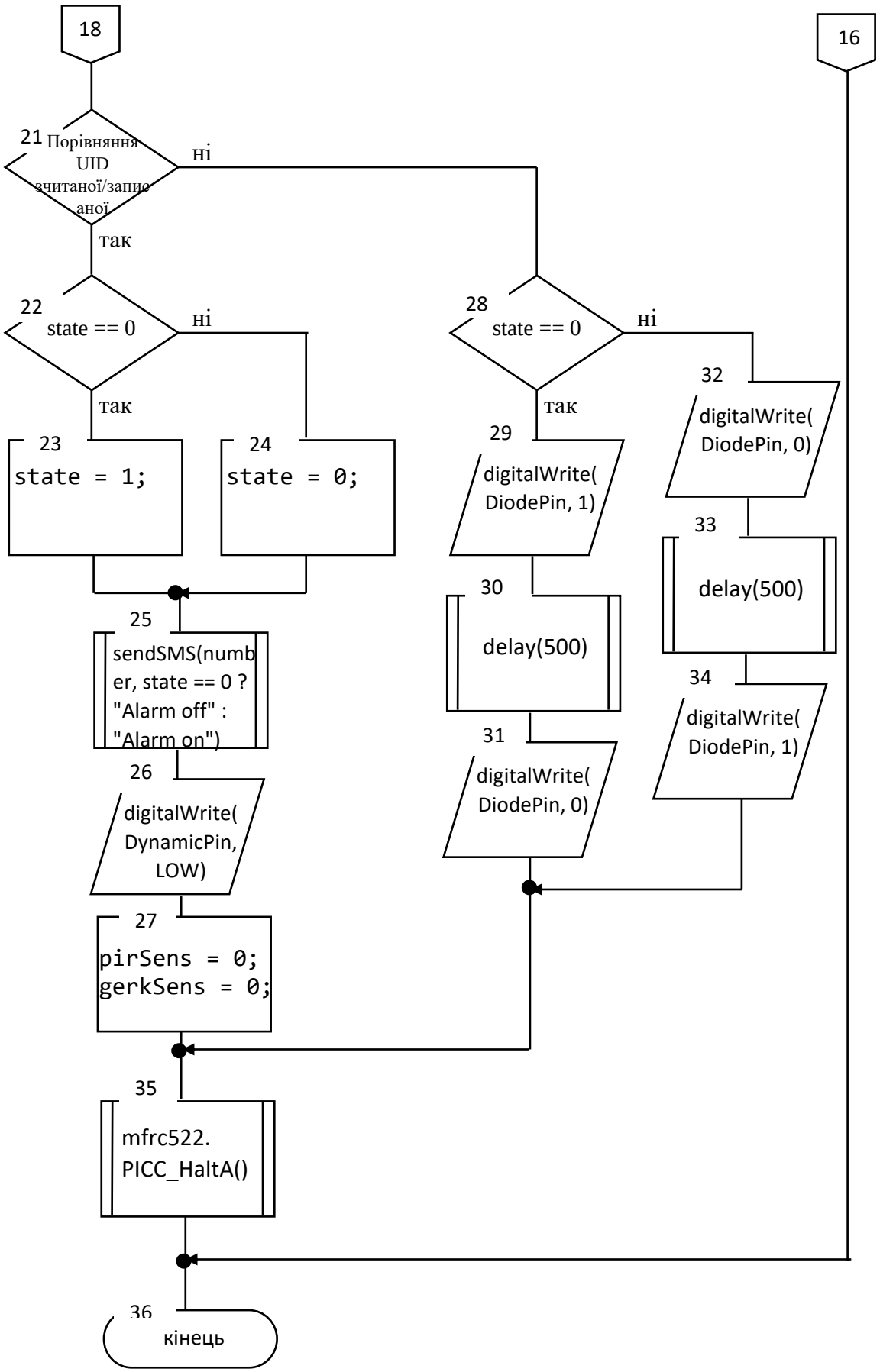
ДОДАТОК В

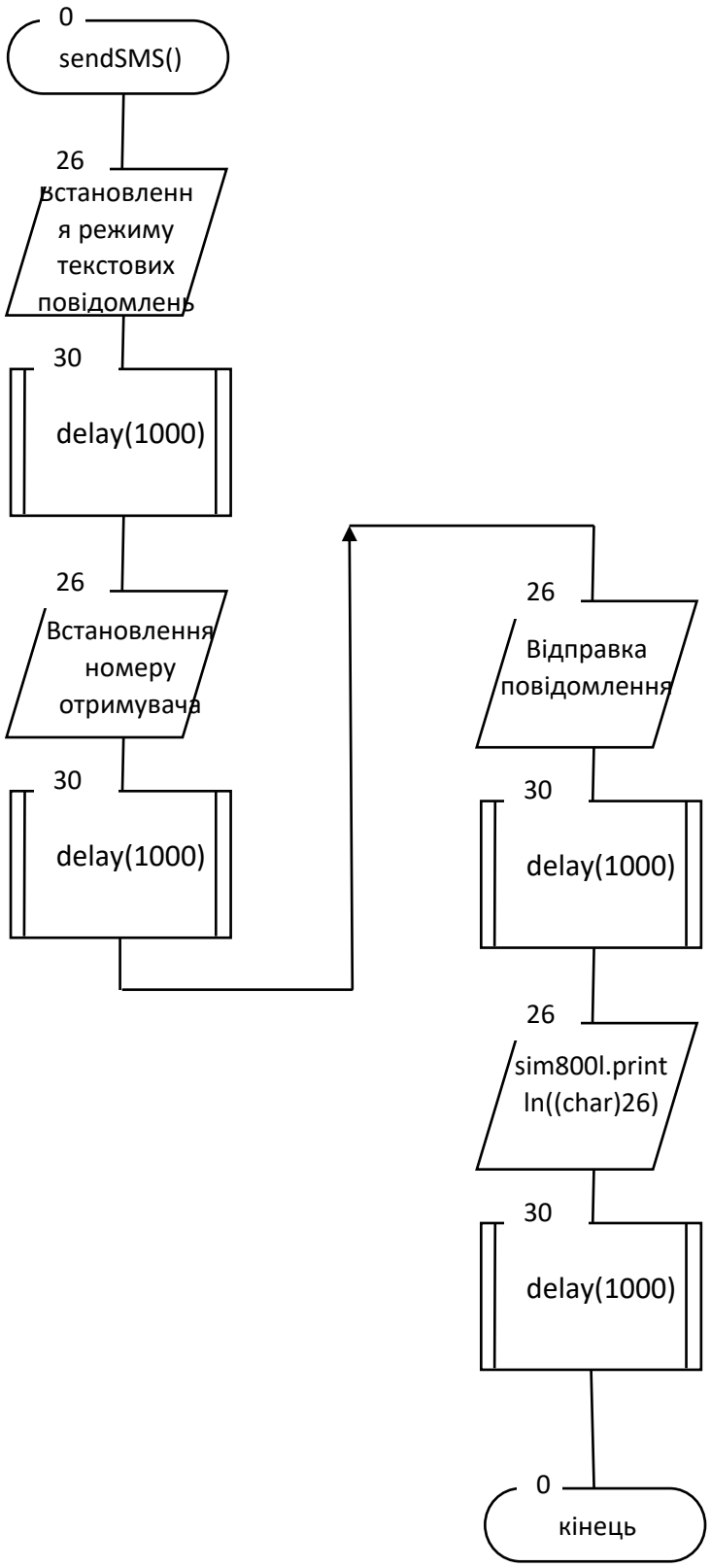
БЛОК СХЕМА АЛГОРИТМУ ПРОГРАМИ




5
6
int DiodePin = 5;
int PIRsensPin = 4;
int GERKsensPin = 3;
int DynamicPin = 2;
7
char savedCardID[] = "13b44f0e";
String number = "+380980001122";
8
sim800l.begin(9600);
SPI.begin();
mfrc522.PCD_ Init();
9
pinMode(DiodePin)
pinMode(PIRsensPin)
pinMode(GERKsensPin)
pinMode(DynamicPin)
10
pirSens = digitalRead(PIRs ensPin)
11
gerkSens = digitalRead(GER KsensPin);
12
Чи помітили датчики рух
ні
так
13
Чи закрита система сигналізації
ні
так
14
16


13
13
14
sendSMS()
15
digitalWrite(
DynamicPin,
HIGH);
16
Картка
піднесена до
зчитувача
ні
так
17
String cardID =
"";
18
byte i = 0;
i <
mfrc522.uid.
size; i++
19
cardID += String(
mfrc522.uid.uidByte
[i] < 0x10 ? "0" :
"");
20
cardID +=
String(mfrc522.uid.
uidByte[i], HEX);
21
36


18
16
21
Порівняння UID зчитаної/запис аної
ні
так
22
state == 0
ні
так
23
state = 1;
24
state = 0;
25
sendSMS(numb er, state == 0 ? "Alarm off" : "Alarm on")
26
digitalWrite(DynamicPin, LOW)
27
pirSens = 0;
gerkSens = 0;
28
state == 0
ні
так
29
digitalWrite(DiodePin, 1)
30
delay(500)
31
digitalWrite(DiodePin, 0)
32
digitalWrite(DiodePin, 0)
33
delay(500)
34
digitalWrite(DiodePin, 1)
35
mfrc522. PICC_HaltA()
36
кінець


0
sendSMS()
26
Встановлення режиму текстових повідомлень
30
delay(1000)
26
Встановлення номеру отримувача
30
delay(1000)
26
Відправка повідомлення
30
delay(1000)
26
sim800l.println((char)26)
30
delay(1000)
0
кінець

ДОДАТОК В
КОД ПРОГРАМИ

```
#include <SPI.h>
#include <MFRC522.h>
#include <SoftwareSerial.h>

bool state = 0;  // змінна що відповідає за стан сигналізації 0 - відкр; 1 - закр;

#define SS_PIN 10
#define RST_PIN 9
MFRC522 mfrc522(SS_PIN, RST_PIN);  // Створюємо об'єкт MFRC522
#define RX_PIN 7
#define TX_PIN 6
SoftwareSerial sim800l(RX_PIN, TX_PIN); // RX, TX піни для з'єднання з модулем SIM800L

int DiodePin = 5;  // записуємо піни для діода, PIR сенсора, геркона та динаміка
int PIRsensPin = 4;
int GERKsensPin = 3;
int DynamicPin = 2;

char savedCardID[] = "13b44f0e";  // Зберігаємо унікальний номер пластикової картки
String number = "+380980001122"; // номер на який будуть надсилатись повідомлення


void setup() {
  sim800l.begin(9600); // Швидкість передачі даних для модуля SIM800L
  SPI.begin();         // Ініціалізуємо шину SPI
  mfrc522.PCD_Init();  // Ініціалізуємо модуль RC522

  pinMode(DiodePin, OUTPUT);  // призначаємо піни для діода, PIR сенсора, геркона та динаміка
  pinMode(PIRsensPin, INPUT);
  pinMode(GERKsensPin, INPUT);
  pinMode(DynamicPin, OUTPUT);

}

void loop() {
```

```
  digitalWrite(DiodePin, state); // оновлюємо стан діода

  //РОБОТА З ДАТЧИКАМИ

  bool pirSens = digitalRead(PIRsensPin);  // зчитування PIR датчику
  bool gerkSens = digitalRead(GERKsensPin);   // зчитування Gerk датчику
  if((pirSens == 1 || gerkSens == 1) && state == 1) // спрацьовування PIR та Gerk датчиків
    {
      sendSMS(number, "Зафіксовано проникнення"); // Повідомляє по СМС про проникнення
      digitalWrite(DynamicPin, HIGH);  // вмикання сирени
    }


  // РОБОТА З КАРТКОЮ

  if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) // Перевіряємо, чи є пластикова картка поблизу
  {
    // Отримуємо унікальний номер пластикової картки
    String cardID = "";
    for (byte i = 0; i < mfrc522.uid.size; i++)
    {
      cardID += String(mfrc522.uid.uidByte[i] < 0x10 ? "0" : "");
      cardID += String(mfrc522.uid.uidByte[i], HEX);
    }


    // Порівнюємо отриманий унікальний номер зі збереженим
    if (cardID.equals(savedCardID))
    {
      state == 0 ? state = 1 : state = 0; // змінюємо стан системи якщо картка підійшла

      sendSMS(number, state == 0 ? "Alarm off" : "Alarm on"); // Повідомляє по СМС стан сигналізації

      digitalWrite(DynamicPin, LOW); // скидуємо тривогу якщо вона активована
      pirSens = 0;
      gerkSens = 0;
    }
    else
```

```
    {
      if(state == 0)   // діод мигне якщо карта не підходить
      {
        digitalWrite(DiodePin, 1);
        delay(500);
        digitalWrite(DiodePin, 0);
      }
      else
      {
        digitalWrite(DiodePin, 0);
        delay(500);
        digitalWrite(DiodePin, 1);
      }
    }

    mfrc522.PICC_HaltA();  // Зупиняємо комунікацію з карткою
  }
}




// відправка СМС повідомлення
void sendSMS(String phoneNumber, String message) {
  sim800l.println("AT+CMGF=1"); // Встановлення режиму текстових повідомлень
  delay(1000);

  sim800l.println("AT+CMGS=\"" + phoneNumber + "\""); // Встановлення номеру
отримувача
  delay(1000);

  sim800l.println(message); // Відправка повідомлення
  delay(1000);

  sim800l.println((char)26); // Код ASCII для Ctrl+Z
  delay(1000);

}
```