КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

інформаційних технологій

(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

на тему: «Розробка апаратно-програмного комплексу охоронної системи підприємства»

Пампуха Микола Миколайович
(прізвище, ім’я та по батькові магістра повністю)

Київ 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

інформаційних технологій

(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ

Тетяна ГОНЧАРЕНКО
„__” _____ 2023 року

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

на тему: «Розробка апаратно-програмного комплексу охоронної системи підприємства»

Виконав: студент 2 – го курсу, групи КН – 1

Спеціальності: 122 «Комп'ютерні науки»

(шифр і назва напряму підготовки, спеціальності)

Магістрант Пампуха Микола Миколайович

(прізвище та ініціали)

Керівник Поплавський О.А .
(прізвище та ініціали)

Рецензент Горда Олена Володимирівна .
(прізвище та ініціали)

Київ, 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій .
Кафедра: інформаційних технологій проектування та ПМ .
Освітній рівень: «магістр за ОПП» .
Спеціальність: 122 «Ком`пютерні науки» .

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ

Тетяна ГОНЧАРЕНКО
„__” _____ 2023 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

---

1. Тема роботи: Розробка апаратно-програмного комплексу охоронної системи підприємства.

затверджена наказом ректора КНУБА № 571/2 від «10» Вересня 2023р.

2. Керівник роботи: Поплавський О.А.
3. Строк подання студентом роботи до захисту: 14 Грудня 2023р.
4. Зміст пояснювальної записки за розділами:

Р.1. Класифікація охоронних систем.
Р.2. Типи охоронних систем.
Р.3. Розрахунки охоронної системи.
Р.4. Проєктування архітектури системи
Р.5. Реалізація системи.

6. Календарний план виконання атестаційної випускної роботи

Види робіт та їх зміст	Дата виконання
Р.1. Класифікація охоронних систем.	01.09.23
Р.2. Типи охоронних систем.	28.09.23
Р.3. Розрахунки охоронної системи.	02.10.23
Р.4. Проєктування архітектури системи	14.10.23
Р.5. Реалізація системи.	01.11.23
Остаточне оформлення роботи	16.11.23
Направлення роботи на рецензування, перевірку на плагіат	24.11.23
Попередній захист роботи на кафедрі	30.11.23

7. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Розділ 1.			
Розділ 2.			
Розділ 3.			
Розділ 4.			
Розділ 5.			

8. Дата видачі завдання: «1» листопада 2022р.

Керівник _____ Поплавський О.А

(підпис) (прізвище та ініціали)

Магістрант _____ Пампуха М.М

(підпис) (прізвище та ініціали)

РЕЗЮМЕ

Київський національний університет будівництва і архітектури

Пампуха Микола Миколайович

факультет автоматизації і інформаційних технологій,

група КН-1

Тема атестаційної випускної роботи: «Розробка апаратно-програмного комплексу охоронної системи підприємства»

освітній рівень: магістр,

спеціальність: 122 «Комп'ютерні науки»,

Науковий керівник: Поплавський О.А

Обсяг роботи. Атестаційна випускова робота магістра складається: розділів 6, стор. 105, таблиць 3, рис. 28, завдання, анотація, вступу, висновків, списку використаних джерел та додатків.

Актуальність теми. Розробка апаратно-програмного комплексу охоронної системи підприємства є актуальною, оскільки питання безпеки підприємств є одними з найважливіших. Охоронні системи використовуються для захисту підприємств від несанкціонованого доступу, крадіжок, пожеж та інших загроз. Зростання рівня злочинності, розвиток нових технологій і зростаюча конкуренція на ринку роблять захист підприємств від несанкціонованого доступу і інших загроз більш актуальним, ніж будь-коли раніше.

У вступі визначені основні напрямки дослідження, обґрунтовано актуальність теми, сформульовано мету та основні завдання системи.

У першому розділі «Розробка апаратно-програмного комплексу охоронної системи підприємства» визначено три основні способи передачі сигналу в охоронних системах. Вибір способу передачі сигналу залежить від таких факторів, як розмір і склад об'єкта, який буде захищатися, тип загроз, від яких необхідно захиститися, фінансові можливості та функціональні вимоги.

У другому розділі «Розробка апаратно-програмного комплексу охоронної системи підприємства» розглядаються основні типи охоронного обладнання, яке використовується для захисту об'єктів від несанкціонованого доступу.

У третьому розділі «Розробка апаратно-програмного комплексу охоронної системи підприємства» розглядаються розрахунки, які необхідно провести для проектування та впровадження охоронної системи. Розрахунки надійності системи дозволяють оцінити, наскільки ймовірно, що система буде працювати без відмови протягом заданого періоду часу. Розрахунки вартості системи дозволяють визначити, скільки коштуватиме розробка, впровадження та експлуатація системи.

У четвертому розділі «Розробка апаратно-програмного комплексу охоронної системи підприємства» розглянуто архітектуру охоронної системи, яка складається з датчиків, контролера та виконавчих пристроїв.

У п'ятому розділі «Розробка апаратно-програмного комплексу охоронної системи підприємства» запропоновано програмно-технічний комплекс практичної реалізації системи, опис класів та функцій програмного засобу, структурна схема програмного комплексу та опис інтерфейсу системи. Також подано приклад розробленої програми у вигляді знімків екранних форм та елементів інтерфейсу. Подано приклад роботи програми.

Ключові слова контролер, сигнал, датчик, надійність, пульт, GSM, бездротовий доступ, провід, вібрація, дим, форма.

Якість оформлення проекту. Атестаційна випускна робота магістра оформлена у відповідності до діючих нормативних документів та методичних вказівок до виконання дипломних робіт для студентів спеціальності 122 «Комп'ютерні науки».Порушень та зауважень під час розробки та перевірки дипломної роботи не виявлено.

Загальний висновок стосовно роботи та присвоєння авторові освітньо-кваліфікаційного рівня «магістр». Робота виконана якісно та на високому рівні, студент продемонстрував достатній рівень теоретичної

підготовки та сформованих практичних навичок в області сучасних інформаційних технологій. Заслуговує оцінки «Відмінно».

Науковий керівник _____/ Поплавський О.А./

(підпис)

Посада, місце роботи: професор кафедри інформаційних технологій проєктування та прикладної математики КНУБА

«23» Листопада 2023р.

АНОТАЦІЯ

Пампуха М.М. «Розробка апаратно-програмного комплексу охоронної системи підприємства».

Атестаційна випускна робота магістра за спеціальністю: 122 «Комп’ютерні науки». – Київський національний університет будівництва та архітектури. – Київ, 2023 р.

Атестаційна робота магістра присвячена створенню апаратно-програмного комплексу охоронної системи підприємства із застосуванням інформаційних технологій. Результатом розробки є програма програмної та апаратної охорони підприємства. Програма надає результати у вигляді тексту.

Ключові слова: контролер, сигнал, датчик, надійність, пульт, GSM, бездротовий доступ, провід, вібрація, дим, форма.

ANNOTATION

Pampukha M.M. "Development of hardware and software complex of the enterprise security system".

Master's thesis for a master's degree in specialty: 122 "Computer Science" - Kyiv National University of Construction and Architecture - Kyiv, 2023.

The master's thesis is devoted to the creation of a hardware and software complex of the enterprise security system using information technology. The result of the development is a program of software and hardware security of the enterprise. The program provides results in the form of text.

Keywords: controller, signal, sensor, reliability, remote control, GSM, wireless access, wire, vibration, smoke, shape.

РЕЦЕНЗІЯ
на атестаційну випускну роботу

Студента Пампухи Миколи Миколайовича
. Факультет автоматизації і інформаційних технологій .
спеціальності 122 «Комп'ютерні науки».

Тема роботи: Розробка апаратно-програмного комплексу охоронної системи підприємства.

Обсяг роботи: атестаційна випускова робота магістра складається: розділів 5, стор. 105, таблиць 3, рис. 28, завдання, анотація, вступу, висновків, списку використаних джерел та додатків.

Висновок про відповідність завданню: робота виконана у повній відповідності до завдання і у встановлений термін .

Актуальність обраної теми:
Розробка апаратно-програмного комплексу (АПК) охоронної системи для підприємства є актуальною і важливою завданням в контексті сучасних викликів у галузі безпеки та управління підприємством.

Використання у роботі сучасних досягнень науки і техніки: розробка проекту базується на використанні сучасних інформаційних комп'ютерних технологій

Використання у роботі комп'ютерних технологій: Visual Studio, C#

Практичне значення роботи: впровадження сучасних інформаційних технологій має забезпечувати виконання ряду вимог, у тому числі наявність зручного і дружнього інтерфейсу, забезпечення безпеки за допомогою різних методів контролю та розмежування доступу до інформаційних ресурсів.

Якість оформлення роботи: випускна робота оформлений у відпо-відності до діючих нормативних документів та методичних вказівок для сту-дентів спеціальності 122

Зауваження та побажання: Зауважень не виявлено

Загальний висновок стосовно роботи та надання авторові освітнього ступеня "магістр": робота виконана на високому рівні, студент продемонстрував високий рівень теоретичної підготовки та сформованих практичних навичок в області сучасних інформаційних технологій. Заслуговує оцінки «відмінно».

Рецензент _____/ _____доц., к.т.н., Горда О.В. ___/
(підпис) (науковий ступінь, вчене звання, прізвище та ініціали)

228

Посада, місце роботи: доцент кафедри інформаційних технологій проєктування та прикладної математики КНУБА
«24» Листопада 2023р.

ЗМІСТ

РОЗДІЛ 1. КЛАСИФІКАЦІЯ ОХОРОННИХ СИСТЕМ

1.1. Способи передачі сигналу в охоронних систем

Способи передачі сигналу в охоронних системах є одним з найважливіших факторів, які слід враховувати при виборі системи для конкретного підприємства. Від способу передачі сигналу залежить швидкість реагування на несанкціонований доступ, надійність системи і її вартість.
Існує три основних способи передачі сигналу в охоронних системах:

- Автономний. При автономній передачі сигналу повідомлення про несанкціонований доступ видається безпосередньо на місці злочину. Це може бути звуковий сигнал, сирена або світлові спалахи. Автономні системи є найпростішими і найдешевшими, але вони також є і найменш ефективними. Вони не забезпечують постійного моніторингу, тому є ризик, що сигнал про несанкціонований доступ не буде помічений.
- Пультовий. При пультовій передачі сигналу повідомлення про несанкціонований доступ передається на пульт охоронної служби. Охорона може швидко відреагувати на сигнал і запобігти злочину. Пультові системи є більш ефективними, ніж автономні, але вони також є і дорожчими.
- GSM. При GSM-передачі сигналу повідомлення про несанкціонований доступ передається на мобільний телефон власника або оператора. Це дозволяє власнику або оператору самостійно відреагувати на сигнал. GSM-системи є більш мобільними, ніж пультові, але вони також є і менш надійними.
-

Автономні системи

Автономні системи не передають сигнал про несанкціонований доступ на пульт охоронної служби. Вони просто видають звуковий сигнал або включають сирену. Автономні системи є найпростішими і найдешевшими, але вони також є і найменш ефективними. Вони не забезпечують постійного моніторингу, тому є ризик, що сигнал про несанкціонований доступ не буде помічений.
Переваги Автономних Систем:

Простота та Надійність: Автономні системи відзначаються своєю простотою в установці та експлуатації. Вони надійні у роботі та не вимагають складних технічних знань для налаштування.

Економічність: Автономні системи зазвичай є більш економічними в порівнянні з іншими методами передачі сигналу. Вони підходять для об'єктів із обмеженим бюджетом, де важлива ефективність при обмежених фінансах.

Невимаганість до Зовнішнього Зв'язку: Оскільки автономні системи видають сигнали безпосередньо на місці злочину, вони не залежать від зовнішнього

зв'язку і не піддаються впливу перебоїв у мобільних мережах або інших комунікаційних систем.

Обмеження Автономних Систем:

Відсутність Постійного Моніторингу: Автономні системи не забезпечують постійного моніторингу об'єкту, що може призвести до непомічення сигналу про несанкціонований доступ, особливо у випадку, коли ніхто не перебуває на місці злочину.

Брак можливості віддаленого керування: Відсутність можливості віддаленого керування може ускладнити управління системою та вимагати фізичної присутності для реагування на події.

Обмежена Функціональність: Деякі автономні системи можуть бути обмежені в своїй функціональності, забезпечуючи лише базовий рівень захисту без додаткових можливостей, таких як віддалений перегляд чи керування.

Пультові системи

Пультові системи передають сигнал про несанкціонований доступ на пульт охоронної служби. Це дозволяє охоронній службі швидко відреагувати на сигнал і запобігти злочину. Пультові системи є більш ефективними, ніж автономні, але вони також є і дорожчими.

Переваги Пультових Систем:

Постійний Моніторинг: Пультові системи забезпечують постійний моніторинг об'єкта, оскільки сигнали про несанкціонований доступ передаються на центральний пульт охорони. Це дозволяє вчасно виявляти та реагувати на будь-які події.

Швидка Реакція: Оператори пульта охорони можуть негайно відреагувати на сигнали та ініціювати відповідні заходи для запобігання злочину чи виявлення порушників.

Можливість Віддаленого Керування: Пультові системи зазвичай дозволяють віддалено керувати системою, включаючи відключення або активацію сигналу, що робить їх гнучкими та зручними у використанні.

Обмеження Пультових Систем:

Вартість: Пультові системи можуть бути високою вартістю, що робить їх менш доступними для об'єктів з обмеженим бюджетом.

Залежність від Інфраструктури: Ефективність пультових систем залежить від стабільної роботи інфраструктури, такої як електропостачання та зв'язок, і може бути обмеженою в разі відмови цих систем.

Необхідність Технічної Підтримки: Установка та обслуговування пультових систем вимагає технічних знань, що може бути проблемою для користувачів без відповідного досвіду.

GSM-системи

GSM-системи передають сигнал про несанкціонований доступ на мобільний телефон власника або оператора. Це дозволяє власнику або оператору самостійно відреагувати на сигнал. GSM-системи є більш мобільними, ніж пультові, але вони також є і менш надійними. Вибір способу передачі сигналу

Переваги ГСМ-систем:

Мобільність та Географічне Охоплення: ГСМ-системи дозволяють власникам та операторам отримувати сповіщення про несанкціонований доступ навіть поза межами підприємства. Це особливо важливо для власників, які часто перебувають в подорожах чи знаходяться в інших локаціях.

Реагування в реальному часі: ГСМ-системи дозволяють власникам безпосередньо реагувати на сигнали про несанкціонований доступ, надаючи можливість прийняти необхідні заходи в реальному часі. Це може значно збільшити шанси на уникнення злочину чи мінімізацію його наслідків.

Віддалений Контроль: ГСМ-системи дозволяють власникам віддалено керувати та моніторити систему, зокрема, відключати або активувати сигнал, отримувати звіти та відстежувати події через мобільний телефон.

Обмеження ГСМ-систем:

Надійність Зв'язку: Незважаючи на мобільність, яка є перевагою, ГСМ-системи можуть зазнавати неполадок в областях з поганим зв'язком або в зонах з обмеженим покриттям, що може зменшити їхню надійність.

Залежність від Мобільної Мережі: ГСМ-системи пов'язані з існуючою мобільною мережею, і їх ефективність може бути обмеженою в разі відмови чи перебоїв в роботі цієї мережі.

Вартість та Плата за Зв'язок: Використання ГСМ-систем може призвести до додаткових витрат на мобільну комунікацію та послуги передачі даних, що може збільшити вартість системи в порівнянні з іншими методами передачі сигналу.

Врахування цих переваг та обмежень допомагає забезпечити оптимальний вибір способу передачі сигналу в охоронній системі з урахуванням конкретних вимог та умов підприємства.
Вибір способу передачі сигналу в охоронних системах залежить від таких факторів:

- Розмір і склад об'єкта, який буде захищатися. Для великих об'єктів з великою кількістю датчиків рекомендується використовувати пультову систему. Для невеликих об'єктів або об'єктів з невеликою кількістю датчиків можна використовувати автономну або GSM-систему.
- Тип загроз, від яких необхідно захиститися. Для захисту від серйозних загроз, таких як крадіжки або пожежі, рекомендується використовувати пультову систему. Для захисту від менш серйозних загроз, таких як спроби незаконного проникнення, можна використовувати автономну або GSM-систему.
- Фінансові можливості. Пультові системи є найбільш дорогими, автономні системи - найдешевшими, а GSM-системи займають проміжне положення.
- Функціональні вимоги. Деякі системи, наприклад, системи з відеоконтролем, передбачають обов'язкову наявність пультового зв'язку.

1.1.2. Типи датчиків в охоронних системах

Датчики є одним з найважливіших компонентів охоронних систем.
Вони відповідають за виявлення несанкціонованого доступу або інших загроз. Існує багато різних типів датчиків, які можна використовувати в охоронних системах. Кожен тип датчика має свої переваги і недоліки.

За способом виявлення загрози датчики можна розділити на такі типи:

- Датчики руху. Датчики руху реагують на рух людини або тварини. Вони є найпоширенішим типом датчиків в охоронних системах.

- Датчики відкриття дверей і вікон. Датчики відкриття дверей і вікон реагують на відкриття дверей і вікон. Вони використовуються для захисту периметра об’єкта.

- Датчики спрацьовування охоронної сигналізації. Датчики спрацьовування охоронної сигналізації реагують на розбиття скла або відкриття сейфа. Вони використовуються для захисту від крадіжок.

- Датчики диму і пожежі. Датчики диму і пожежі реагують на появу диму або пожежі. Вони використовуються для захисту від пожеж.

- Датчики витоку води. Датчики витоку води реагують на витік води. Вони використовуються для захисту від затоплення.

- Датчики землетрусу. Датчики землетрусу реагують на землетрус. Вони використовуються для захисту від руйнувань.

За способом монтажу датчики можна розділити на такі типи:

- Провідні датчики. Провідні датчики з'єднані з контролером за допомогою проводів. Вони є більш надійними, ніж бездротові датчики, але вони також є і більш дорогими.

- Бездротові датчики. Бездротові датчики з'єднані з контролером за допомогою радіосигналу. Вони є більш мобільними, ніж провідні датчики, але вони також є і менш надійними.

За способом управління датчики можна розділити на такі типи:

- Активні датчики. Активні датчики випромінюють сигнал, який відбивається від об'єкта, що рухається.

- Пасивні датчики. Пасивні датчики реагують на зміни в навколишньому середовищі, викликані рухом об’єкта.

Вибір датчиків

Вибір датчиків для охоронної системи залежить від таких факторів:

- Тип загрози, від якої необхідно захиститися. Для захисту від різних загроз використовуються різні типи датчиків.

- Розмір і склад об'єкта, який буде захищатися. Для великих об'єктів з великою кількістю дверей і вікон рекомендується використовувати датчики відкриття дверей і вікон. Для невеликих об'єктів або об'єктів з невеликою кількістю дверей і вікон можна використовувати датчики руху.

- Фінансові можливості. Провідні датчики є більш дорогими, ніж бездротові датчики.

- Функціональні вимоги. Деякі системи, наприклад, системи з відеоконтролем, передбачають обов'язкову наявність певних типів датчиків.

Технологічні Інновації у Сфері Датчиків в Охоронних Системах

З розвитком технологій постійно з'являються нові можливості для поліпшення функціональності охоронних систем. Інновації у сфері датчиків відкривають нові перспективи для ефективного виявлення та реагування на потенційні загрози.

Використання Штучного Інтелекту (ШІ) в Датчиках:
Введення штучного інтелекту у датчики дозволяє їм аналізувати збір інформації більш ефективно. Датчики, обладнані ШІ, можуть розпізнавати зразки та аномалії, адаптовувати свою роботу до змін у середовищі та навіть прогнозувати можливі загрози на основі аналізу великих обсягів даних.

Інтеграція Датчиків та Систем Відеоспостереження:
Поєднання датчиків руху з системами відеоспостереження дозволяє забезпечити комплексний підхід до охорони. Датчики можуть ініціювати включення відеокамер у випадках виявлення руху, а системи відеоспостереження в свою чергу дозволяють візуалізувати ситуацію та вчасно реагувати на потенційні загрози.

Застосування Технологій Розпізнавання Облич та Об'єктів:
Вбудовані системи розпізнавання облич і об'єктів у датчиках можуть вдосконалити точність виявлення загроз. Ця технологія дозволяє автоматично розпізнавати і класифікувати об'єкти, що може бути корисним у виявленні непередбачених сценаріїв.

Використання Наноматеріалів у Датчиках:
Застосування наноматеріалів у виробництві датчиків може покращити їхню чутливість та стійкість. Нанодатчики можуть бути більш ефективними виявниками різних видів загроз, включаючи гази, хімічні сполуки та інші небезпечні речовини.

Інтеграція Засобів Інтернету Речей (IoT) у Датчики:
Включення датчиків до системи Інтернету речей розширює можливості моніторингу та віддаленого керування. Це дозволяє отримувати реальний час інформації та віддалено керувати охоронними системами через мобільні пристрої.

Переваги та Обмеження Інновацій у Датчиках в Охоронних Системах
Переваги
Підвищена Чутливість та Точність: Інновації в датчиках дозволяють підвищити їхню чутливість та точність виявлення загроз, зменшуючи ймовірність помилок та ложних сигналів.
Збільшена Автономія та Ефективність: Використання ШІ та IoT робить датчики більш автономними та забезпечує ефективний обмін інформацією без значного втручання користувача.
Комплексний Підхід до Охорони: Інтеграція різних видів датчиків та їхніх функцій дозволяє створювати комплексні системи, що забезпечують більш повне охоплення захисту.

Обмеження:

Високі Витрати на Впровадження: Впровадження інновацій у датчики може бути пов'язане із великими витратами, особливо у випадку використання новітніх матеріалів та технологій.
Потреба в Високотехнологічній Технічній Підтримці: Сучасні датчики потребують високотехнологічної технічної підтримки, що може бути складним для забезпечення у випадку відсутності відповідних кадрів.
Питання Приватності та Безпеки Даних: Використання технологій розпізнавання облич та IoT може породжувати питання щодо приватності та безпеки обробки та зберігання особистих даних.

1.1.3. Класифікація за конструктивними та іншими ознаками

Охоронні системи можна класифікувати за різними ознаками.
За конструктивними ознаками охоронні системи поділяються на такі типи:

- Провідні системи. У провідних системах датчики і контролер з'єднані між собою проводами.
- Бездротові системи. У безпровідних системах датчики і контролер з'єднані між собою за допомогою бездротового зв'язку.

За способом передачі сигналу охоронні системи поділяються на такі типи:

- Автономні системи. У автономних системах сигнал про несанкціонований доступ видається безпосередньо на місці злочину.
- Пультові системи. У пультових системах сигнал про несанкціонований доступ передається на пульт охоронної служби.
- GSM-системи. У GSM-системах сигнал про несанкціонований доступ передається на мобільний телефон власника або оператора.

За типом датчиків охоронні системи поділяються на такі типи:

- Датчики руху. Датчики руху реагують на рух людини або тварини.
- Датчики відкриття дверей і вікон. Датчики відкриття дверей і вікон реагують на відкриття дверей і вікон.
- Датчики спрацьовування охоронної сигналізації. Датчики спрацьовування охоронної сигналізації реагують на розбиття скла або відкриття сейфа.
- Датчики диму і пожежі. Датчики диму і пожежі реагують на появу диму або пожежі.
- Датчики витоку води. Датчики витоку води реагують на витік води.
- Датчики землетрусу. Датчики землетрусу реагують на землетрус.

За способом монтажу охоронні системи поділяються на такі типи:

- Централізовані системи. У централізованих системах всі датчики підключені до одного контролера.
- Децентралізовані системи. У децентралізованих системах кожен датчик має свій контролер.

За функціональними можливостями охоронні системи поділяються на такі типи:

- Основні системи. Основні системи забезпечують виявлення несанкціонованого доступу.

- Розширені системи. Розширені системи забезпечують додаткові функції, такі як відеоспостереження, контроль доступу, управління освітленням і т.д.

За сферою застосування охоронні системи поділяються на такі типи:

- Для підприємств. Охоронні системи для підприємств призначені для захисту підприємств від несанкціонованого доступу, крадіжок, пожеж та інших загроз.
- Для житлових будинків. Охоронні системи для житлових будинків призначені для захисту житлових будинків від несанкціонованого доступу, крадіжок і інших злочинів.
- Для транспортних засобів. Охоронні системи для транспортних засобів призначені для захисту транспортних засобів від крадіжок і інших злочинів.

Додаткові ознаки класифікації

Крім основних ознак, охоронні системи можна класифікувати за такими додатковими ознаками:

- За способом розміщення датчиків. Охоронні системи можуть бути внутрішніми або зовнішніми.
- За способом управління. Охоронні системи можуть бути ручними або автоматичними.
- За принципом роботи. Охоронні системи можуть бути контактними або безконтактними.
- За надійністю. Охоронні системи можуть бути високонадійними, середньонадійними або низьконадійними.
- За вартістю. Охоронні системи можуть бути дорогими, середньовартісними або дешевими.
- За конструктивними ознаками можна виділити ще один важливий тип охоронних систем — гібридні системи. Гібридні системи об'єднують в собі як провідні, так і бездротові технології. Це дозволяє досягти оптимального балансу між надійністю провідних систем і гнучкістю бездротових. Такий підхід особливо корисний у великих об'єктах або в тих випадках, коли проведення кабельної інфраструктури є трудомістким завданням.
-
- За способом передачі сигналу можна виокремити ще один важливий тип — Інтернет-системи. У цих системах датчики та контролери підключені до Інтернету, що відкриває широкі можливості для віддаленого моніторингу та управління. Вони можуть бути використані для захисту від кібератак, а також для отримання доступу до інформації в режимі реального часу.
-

- Щодо типу датчиків, слід зазначити, що мультисенсорні системи стають все більш популярними. Ці системи об'єднують кілька видів датчиків в одному пристрої, що дозволяє забезпечити більш широкий спектр виявлення загроз і подій. Наприклад, мультисенсорні датчики можуть одночасно реагувати на рух, зміни температури, та виток води, що робить їх універсальними у різноманітних умовах.

- За способом монтажу можна виділити ще одну категорію — розподілені системи. У розподілених системах датчики та контролери розташовані на різних частинах об'єкта, що дозволяє забезпечити більш ефективне охоплення території та швидшу реакцію на події в різних зонах.

- За функціональними можливостями, важливо відзначити інтегровані системи безпеки. Ці системи поєднують в собі не лише виявлення загроз, але й можливості взаємодії з іншими системами, такими як системи автоматизації, освітлення та контролю доступу. Такий підхід забезпечує комплексний підхід до безпеки об'єкта.

- За сферою застосування варто відзначити охоронні системи "розумного будинку". Ці системи не лише виконують функції безпеки, а й забезпечують зручність та енергоефективність для мешканців. Вони можуть автоматично регулювати освітлення, температуру, та інші параметри в приміщенні, створюючи оптимальне та комфортне середовище.

- Ще однією важливою додатковою ознакою є системи реакції на екстремальні ситуації. Охоронні системи, які включають в себе можливості автоматичної реакції на надзвичайні ситуації, такі як пожежа чи землетрус, стають дедалі більш важливими в умовах зростаючого ризику природних катастроф.

1.1.4. Юридичний аспект

Законодавство України, що регулює сферу охоронних систем, визначає не лише обов'язки охоронних організацій та власників об'єктів, а й встановлює правові, економічні та технічні стандарти для забезпечення ефективної охорони власності та безпеки громадян. Однією з ключових нормативних баз є "Закон України "Про охоронну діяльність", який визначає основні принципи та порядок здійснення охоронної діяльності.

Постанова Кабінету Міністрів України від 24 жовтня 2012 року № 1070 "Про затвердження Правил охорони об'єктів, що охороняються орендарями, наймателями або іншими суб'єктами господарювання" становить важливий

документ, який регулює порядок охорони об'єктів, перебуваючи на балансі орендарів чи наймачів. Це включає в себе визначення вимог до систем безпеки та обов'язки суб'єктів господарювання.

Окремо слід звернутися увагу на Постанову Кабінету Міністрів України від 10 жовтня 1992 року № 576 "Про затвердження Положення про охоронні підприємства", яке визначає порядок створення, діяльності та реорганізації охоронних підприємств. Цей документ встановлює стандарти в галузі професійної підготовки охоронців, а також визначає їхні права та обов'язки.

Основні вимоги до охоронних систем, які законодавство визначає, стосуються якості та надійності. Системи повинні відповідати встановленим нормам і стандартам, проходити сертифікацію, а також забезпечувати високий рівень захисту інформації.

Зобов'язання власника чи орендодавця об'єкта, який охороняється, не обмежуються лише фінансовими аспектами. Вони також полягають у забезпеченні належного технічного стану охоронної системи та наданні доступу для проведення технічного обслуговування та ремонту. Це є важливою умовою для забезпечення безперебійної роботи системи та максимального рівня захисту.

Охоронні організації, в свою чергу, мають виконувати ряд обов'язків для ефективного функціонування охоронних систем. Проведення своєчасного технічного обслуговування, реагування на сигнали тривоги та збереження інформації — це лише декілька з аспектів, які вони повинні враховувати. Важливо, щоб охоронні організації були готові до будь-яких викликів і забезпечували надійний захист об'єктів.

Порушення вимог законодавства у сфері охорони об'єктів може призвести до серйозних наслідків для власників, орендарів та охоронних організацій. Передбачена адміністративна та кримінальна відповідальність створює стимул для відповідального та професійного підходу до впровадження та експлуатації охоронних систем.

При розробці апаратно-програмного комплексу охоронної системи для підприємства, необхідно не лише враховувати технічні аспекти, але й дотримуватися усіх юридичних норм. Це дозволить створити не лише ефективну систему безпеки, а й уникнути можливих юридичних проблем у майбутньому.

Для успішної реалізації проекту важливо вивчити не лише технічні можливості охоронних систем, а й їхню відповідність законодавству. Дотримання усіх вимог і стандартів дозволить не тільки забезпечити безпеку об'єкта, а й стати дієвим і високошвидкісним інструментом для виявлення та реагування на потенційні загрози.

Законодавче поле, що регулює охоронні системи в Україні, постійно змінюється, щоб адаптуватися до сучасних технологій та вимог безпеки. Важливим аспектом є також удосконалення систем сертифікації охоронних засобів, яке враховує нові технології та стандарти безпеки.

З іншого боку, наукові та технічні досягнення в області інформаційної безпеки та технічних рішень для охоронних систем надають нові можливості для захисту об'єктів. Використання штучного інтелекту, аналізу великих обсягів даних та розширеної реальності стає все більш актуальним у контексті розробки сучасних охоронних систем.

Застосування новітніх технологій також може сприяти розвитку інтегрованих систем безпеки, які поєднують в собі не лише фізичну, але й кібербезпеку. Це важливо, зокрема, у контексті захисту від кібератак, які можуть спрямовуватися не лише на інформаційні системи, а й на фізичні об'єкти та пристрої.

Важливим аспектом розгляду є також міжнародні стандарти та норми, які регулюють сферу охоронних систем. Адаптація та впровадження таких стандартів сприяє взаємодії з міжнародними партнерами та забезпечує високий рівень якості та безпеки охоронних систем на національному рівні.

Однак важливо враховувати етичні та приватні аспекти використання охоронних систем. Збір та обробка великої кількості інформації може викликати питання щодо приватності та використання даних. З цього приводу виникає потреба в розробці та дотриманні етичних стандартів у сфері використання технологій безпеки.

Невід'ємною частиною розвитку охоронних систем є інноваційний підхід до вирішення проблем безпеки. Співпраця між вченими, інженерами та представниками бізнесу сприяє створенню нових технологій та методів, що поліпшують якість та ефективність охоронних систем.

У заключенні, розвиток сучасних охоронних систем є багатограннім завданням, яке потребує комплексного підходу та урахування різноманітних аспектів, починаючи від законодавчого регулювання та закінчуючи використанням передових технологій та етичних стандартів
.

РОЗДІЛ 2. ТИПИ ОХОРОННИХ СИСТЕМ

2.1. Датчики руху

Принцип роботи датчиків руху

Датчики руху працюють на основі різних принципів. Інфрачервоні датчики руху використовують інфрачервоне випромінювання для виявлення руху. Коли людина або тварина проходять повз датчик, вони відбивають інфрачервоне випромінювання, яке фіксується датчиком.

Магнітоконтактні датчики руху використовують магнітне поле для виявлення руху. Коли людина або тварина переміщаються, вони порушують магнітне поле, яке фіксується датчиком.

Ультразвукові датчики руху представляють собою ще один тип сучасних пристроїв, які використовуються для виявлення руху. Ці датчики використовують високочастотні звукові хвилі, які не чутні для людини, для створення невидимого "звукового бар'єру". Коли об'єкт перетинає цей бар'єр, звукові хвилі відбиваються від об'єкта і сприймаються датчиком. Такий метод дозволяє точно визначити наявність руху та його напрямок.

Відеодатчики руху стають все популярнішими завдяки розвитку відеоспостереження. Вони використовують вбудовані або підключені камери для виявлення змін в зображенні. Алгоритми обробки зображення дозволяють виявити рух об'єктів та визначити їхні розміри та швидкість. Відеодатчики руху особливо ефективні в широких просторах, таких як парковки чи склади, де потрібно виявляти рух на великій площі.

Рис. 2.1. Датчик руху.

Мікрохвильові датчики руху використовують електромагнітні хвилі з високою частотою для виявлення руху об'єктів. Вони можуть працювати в різних погодних умовах та не залежать від освітлення навколишнього середовища. Коли об'єкт перетинає зону дії мікрохвильового датчика, змінюється час, за який хвилі повертаються до датчика, і це фіксується як рух.

Акустичні датчики руху використовують звукові хвилі для виявлення руху об'єктів. Ці датчики можуть використовувати як ультразвук, так і акустичні сигнали, щоб виявляти зміни в оточуючому середовищі. Зазвичай вони використовуються в приміщеннях, де звукові хвилі можуть ефективно взаємодіяти з стінами та перешкодами.

Радіочастотні ідентифікатори (RFID) також можуть використовуватися для виявлення руху, зокрема в системах безпеки. Кожен об'єкт чи особа, які мають RFID-мітки, можуть бути ідентифіковані, коли вони перетинають зону дії читача RFID. Цей метод ефективний для контролю доступу та виявлення руху об'єктів у визначених зонах.

Інтеграція датчиків руху у різні типи охоронних систем робить їх більш надійними та ефективними. Завдяки поєднанню різних технологій, можливе створення систем, які адаптуються до різноманітних умов та вимог безпеки. Разом із зростанням обчислювальної потужності та розвитком сучасних алгоритмів обробки даних, датчики руху стають не лише елементом безпеки, але й ключовою частиною розумних систем управління та моніторингу.

Класифікація датчиків руху

Класифікація датчиків руху відображає різноманітність технологій та принципів їхньої роботи, що сприяє вибору оптимального рішення для конкретної системи безпеки.

Однією з ключових ознак є принцип роботи датчика руху. Інфрачервоні датчики використовують теплове випромінювання об'єктів для виявлення руху. Активні інфрачервоні датчики випромінюють сигнал і вимірюють його відбиття, визначаючи наявність руху. Пасивні датчики реагують на зміни температури в навколишньому середовищі, сприймаючи теплове випромінювання.

Ще однією важливою характеристикою є тип випромінювання, яке використовується датчиком. Датчики можуть використовувати інфрачервоне, ультрафіолетове, радіо- або мікрохвильове випромінювання. Інфрачервоні датчики є найпоширенішими, оскільки вони ефективні та економічні.

За способом монтажу датчики можна поділити на провідні та бездротові. Провідні датчики з'єднані з центральною системою за допомогою кабелів, що робить їх стійкими до перешкод та електромагнітних впливів. Бездротові датчики, навпаки, забезпечують більшу гнучкість в розташуванні, але можуть бути менш надійними через можливість перешкод для сигналу.

За типом зони розпізнавання і дії датчики поділяються на зонові та об'єктові. Зонові датчики контролюють певну область, і будь-яке порушення в цій зоні викликає тривогу. Об'єктові датчики визначають рух або відсутність руху конкретного об'єкта, і тільки в цьому випадку спрацьовує тривога.

Розглядаючи класифікацію датчиків руху, слід враховувати інші фактори, такі як чутливість, ступінь захищеності від атмосферних впливів та можливості маскування. Вибір конкретного типу датчика руху повинен враховувати особливості конкретного об'єкта та завдання системи безпеки.

Особливу увагу слід приділяти високотехнологічним рішенням, що поєднують в собі кілька принципів роботи. Наприклад, інтеграція інфрачервоного та ультразвукового датчиків може забезпечити ефективний контроль за рухом в різних умовах, забезпечуючи високу точність та надійність системи безпеки.
Технологічні інновації в галузі датчиків руху надають можливості для подальшого розвитку систем безпеки. Однією з передових тенденцій є використання технологій штучного інтелекту (ШІ), які дозволяють датчикам аналізувати зібрані дані та вдосконалювати свою реакцію на різноманітні сценарії.

Розвиток "розумних" датчиків руху передбачає їх здатність взаємодіяти та адаптуватися до змін у середовищі. Наприклад, датчики можуть визначати тип об'єкта, що рухається (людина, транспортний засіб, тварина) і враховувати цю інформацію для вибору оптимальної стратегії взаємодії з системою безпеки.

Крім того, розширені можливості використання датчиків руху в системах "розумного будинку" та "розумного офісу" стають актуальними. Датчики можуть реагувати на рух та автоматично керувати освітленням, системами кондиціювання повітря та іншими аспектами оточуючого середовища, забезпечуючи комфорт та ефективність.

Окрім того, сучасні датчики руху стають невидимими та естетично прийнятними в екстер'єрі об'єктів. Мініатюрні розміри та висока точність роботи роблять їх ідеальним вибором для використання в будь-яких архітектурних рішеннях, забезпечуючи безпеку без порушення естетики.

У світлі технологічних змін і вдосконалення датчиків руху, також постає питання їх етичного використання. Збір та обробка великої кількості

інформації може породжувати питання приватності та безпеки даних. Сучасна наука та законодавство повинні враховувати ці аспекти та визначати правила використання таких технологій.

Загалом, класифікація датчиків руху відкриває широкий простір для подальших досліджень і розвитку. Сполучення різних технологій, їх

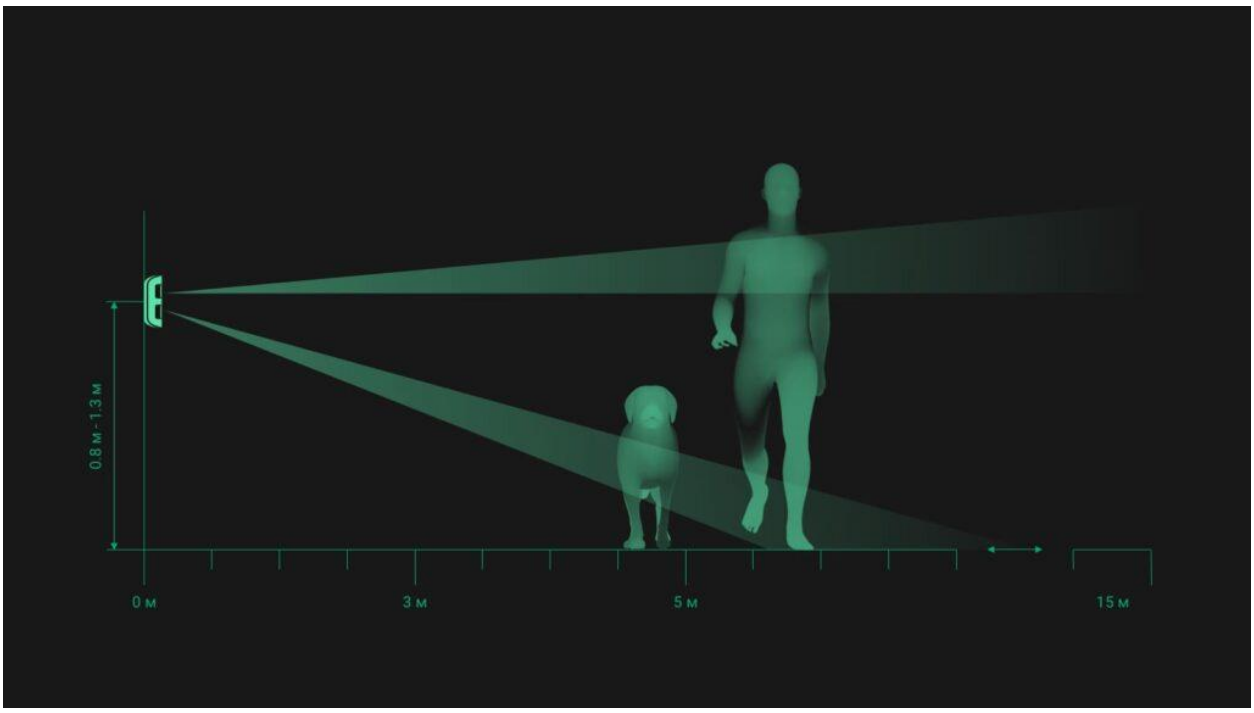


Рис. 2.2. Візуалізація магнітного поля для виявлення руху.

ефективне використання та врахування вимог ринку та суспільства роблять цю галузь ключовою для забезпечення безпеки, зручності та ефективності в різних сферах життя.

За принципом роботи датчики руху можна розділити на:

- Інфрачервоні датчики руху
- Магнітоконтактні датчики руху
- Електромагнітні датчики руху
- Датчики руху на основі ультразвуку

За способом монтажу датчики руху можна розділити на:

- Настінні датчики руху
- Стельові датчики руху
- Поворотні датчики руху

Рис. 2.3. Настінний датчик руху

Рис. 2.4. Стельовий датчик руху

Рис. 2.5. Поворотній датчик руху

Переваги та недоліки датчиків руху

Висока ефективність: Датчики руху надзвичайно ефективні в виявленні навіть маленьких рухів, що робить їх ефективними в системах безпеки та автоматизації.

Простота монтажу: Встановлення датчиків руху в основному не вимагає складних технічних навичок. Це дозволяє використовувати їх широко як вдома, так і в комерційних об'єктах.

Невисока вартість: Більшість датчиків руху доступні за помірну ціну, що робить їх доступними для широкого кола користувачів та підприємств.

Недоліки датчиків руху:

Можливі помилкові спрацьовування: Датчики руху можуть реагувати на непередбачувані фактори, такі як тварини, літаючі об'єкти або рухаючіся тіні, що може спричинити помилкові сигнали тривоги.

Неможливість виявлення руху всередині приміщення: Традиційні датчики руху, які базуються на інфрачервоному випромінюванні, можуть бути менш ефективними виявлення руху всередині приміщення через обмежені можливості проникнення сигналу через стіни та перешкоди.

Обмежений радіус дії: Більшість датчиків руху мають обмежений радіус дії, і їхні можливості можуть бути обмежені фізичними характеристиками приміщення або встановленої області.

Потреба в джерелі живлення: Деякі типи датчиків руху потребують постійного джерела енергії, що може бути не зручно в умовах, де важко забезпечити стабільне електроживлення.

Застосування та розвиток датчиків руху:

Удосконалення алгоритмів розпізнавання: Подальший розвиток в галузі штучного інтелекту та машинного навчання може поліпшити алгоритми розпізнавання руху та зменшити кількість помилкових спрацьовувань.

Використання технології радарів: Впровадження радарів для роботи в датчиках руху може покращити їхню точність та здатність виявлення руху навіть ускладнених умовах.

Розширення бездротових можливостей: Застосування технології бездротового зв'язку дозволяє розширити область використання датчиків руху та полегшити їхню установку та обслуговування.

Інтеграція з "розумними" системами: Поєднання датчиків руху з іншими "розумними" системами, такими як системи відеоспостереження, може значно покращити здатність систем безпеки реагувати на різні ситуації.

Вибір датчика руху

При виборі датчика руху необхідно враховувати такі фактори, як:

- Тип приміщення, яке потрібно захистити
- Мета захисту
- Бюджет

Вплив типу приміщення на вибір датчика руху:

Тип приміщення, в якому буде встановлений датчик руху, є ключовим фактором при виборі певного пристрою. Наприклад, для використання в житловому приміщенні може бути обрано датчики руху, які не реагують на домашніх тварин чи невеликі рухи, зменшуючи тим самим кількість помилкових спрацювань. У комерційних будівлях можуть вимагатися більш продуктивні та точні датчики руху, спроможні виявляти навіть найменші рухи для забезпечення високого рівня безпеки.

Врахування мети захисту:

Визначення конкретної мети використання датчика руху грає ключову роль у виборі відповідного пристрою. Наприклад, якщо основною метою є захист від несанкціонованого доступу, то обрані датчики повинні бути спроможні виявляти навіть найменший рух. У випадку використання для системи енергозбереження важливим може бути визначення активності в зоні, щоб вмикати чи вимикати освітлення або системи кондиціювання повітря.

Вплив бюджету на вибір датчика руху:

Бюджет визначає межі вибору технічного обладнання. Для економічно обґрунтованого підходу до безпеки можуть вибиратися більш доступні вартісно датчики руху, які пропонують базові функції. З іншого боку, високобюджетний проект може дозволити вибір технологічно складніших пристроїв з розширеними функціональними можливостями, такими як інтеграція з системами "розумного" будинку чи аналітика даних руху для оптимізації просторового планування.

Технічні можливості датчика руху:

Основні технічні характеристики, які важливі при виборі датчика руху, включають дальність виявлення, кут огляду, чутливість до руху, а також можливості вирізняти між різними типами рухливих об'єктів. Наприклад, для широких приміщень можуть бути вибрані датчики руху з більшим кутом огляду, тоді як для вузьких коридорів важливою може бути точність виявлення на великій дистанції.

Системи безпеки та їх інтеграція:

Вибір датчика руху також залежить від того, як він інтегрується з існуючими або плануваними системами безпеки. Здатність взаємодіяти з системами відеоспостереження, контролю доступу чи централізованими системами моніторингу може бути вирішальною для створення повноцінної системи безпеки.

Врахування екологічних умов:

Деякі датчики руху можуть бути більш адаптованими до конкретних екологічних умов. Наприклад, деякі пристрої підходять для використання в умовах високої вологості чи низьких температур, що робить їх ідеальними для встановлення на вулиці або в неопалюваних приміщеннях.

Заключні висновки при виборі:

Обговорені фактори взаємодіють між собою, вимагаючи уважного аналізу та збалансованого підходу. Ефективний вибір датчика руху передбачає врахування всіх зазначених аспектів, а також пошук оптимального компромісу між функціональністю, технічними характеристиками та фінансовими можливостями.

Рис. 2.6. Датчик за 60 грн

Рис. 2.7. Датчик за 9000 грн

Рис. 2.8. Датчик з лампою

Встановлення датчиків руху

Датчики руху повинні встановлюватися відповідно до інструкції виробника. При установці датчиків руху необхідно враховувати такі фактори, як:

- Вісь датчика повинна бути спрямована в точку найбільш ймовірного проникнення
- Датчик повинен бути встановлений на висоті не менше 2 метрів

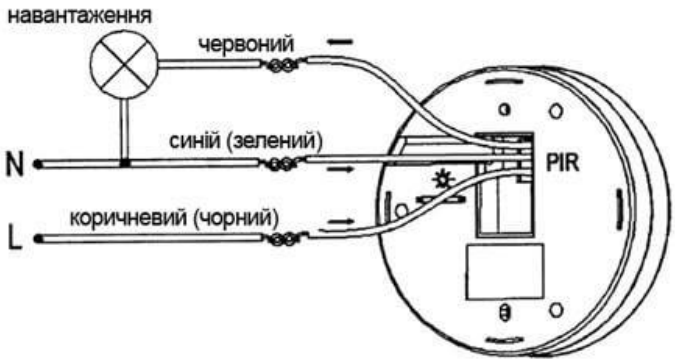


Рис. 2.9. Схема підключення датчику

- Вибір оптимального місця для встановлення датчиків руху є ключовим етапом в створенні ефективної системи безпеки. Це вимагає ретельного вивчення особливостей об'єкта та зон, які потрібно контролювати. Зокрема, важливо визначити напрямок руху можливих загроз, розташування цінних об'єктів, а також особливості освітлення.
- Орієнтація вісі датчика у напрямку найбільш ймовірного проникнення допомагає максимально використовувати його потенціал. Наприклад,

якщо датчик руху встановлено для виявлення вторгнень через вхідні двері, важливо спрямувати його вздовж шляху, яким ймовірно проникнення. Це дозволить системі виявити порушення безпеки на ранніх етапах та надати можливість вчасно реагувати.

- Встановлення датчиків на висоті не менше 2 метрів є стандартним правилом і має свої важливі переваги. На такій висоті датчики мають кращий огляд навколишнього простору, запобігаючи випадковим спрацюванням внаслідок дій тварин або дітей. Вище розташований датчик також складніше недоступний для несанкціонованого втручання.

- Важливо також звертати увагу на зону покриття датчика та його чутливість. Оптимальною є установка таких датчиків, що вони покривають велику площу, але при цьому можуть реагувати на найменші рухи. Наприклад, у зоні з обмеженим освітленням можуть використовуватися датчики, обладнані інфрачервоними світлодіодами, які дозволяють виявляти рух в темряві.

- Установка зон розпізнавання і врахування характеристик об'єктів. Розгляньте можливість встановлення декількох датчиків для покриття різних зон та уточнення їхніх параметрів в залежності від конкретних потреб. Наприклад, на відкритих площах можуть бути використані датчики з високою чутливістю, тоді як для приміщень із великою кількістю перешкод можна встановити багатозонові датчики з регульованою зоною дії.

- Розгляд можливості використання "умілих" датчиків, що можуть адаптуватися до змін у середовищі. Такі датчики можуть самостійно регулювати свою чутливість та зону дії в залежності від часу доби, погоди чи інших умов. Це збільшує точність реагування системи та зменшує ймовірність спрацювання від факторів, які не є загрозою безпеці.

- Технологічні рішення для підвищення надійності. Інтеграція технологій, таких як маскування та антитамперна захист, дозволяє підвищити стійкість системи до спроб обхіду або вимкнення датчика. Маскування полягає в умисному прихованні датчика, щоб зробити його менш помітним для потенційних порушників.
Технологічні рішення для підвищення надійності:

Інтеграція технологій, таких як маскування та антитамперна захист, дозволяє підвищити стійкість системи до спроб обхіду або вимкнення датчика. Маскування полягає в умисному прихованні датчика, щоб зробити його менш помітним для потенційних порушників. Це ускладнює завдання тим, хто може намагатися обійти систему, забезпечуючи додатковий рівень безпеки.

Врахування цих аспектів при встановленні датчиків руху допомагає не лише забезпечити найвищий рівень безпеки, але й підвищити ефективність та надійність всієї системи. Здійснення обґрунтованого вибору місця та правильної конфігурації датчиків руху є вирішальним етапом у забезпеченні ефективної охорони будь-якого об'єкта.
Професійне консультування і підготовка персоналу:

Здійснення вибору та правильної установки датчиків руху варто проводити під керівництвом фахівців. Професійне консультування спеціалістів в галузі безпеки дозволяє врахувати специфіку об'єкта, його розташування, а також види можливих загроз.

Крім того, надається акцент на необхідності підготовки персоналу, який буде відповідати за експлуатацію та моніторинг системи безпеки. Особи, відповідальні за цей процес, повинні бути ознайомлені з принципами роботи датчиків, а також навчені виявляти та реагувати на можливі неполадки чи аварійні ситуації.

Інтеграція з іншими системами безпеки:

Для максимальної ефективності система датчиків руху повинна інтегруватися з іншими засобами безпеки, такими як системи відеоспостереження, контролю доступу та вогневого захисту. Взаємодія цих систем створює комплексний підхід до безпеки об'єкта.

Наприклад, в разі спрацювання датчика руху система відеоспостереження може автоматично спрямовувати камери в потрібний сектор для отримання деталізованих зображень та відстеження події в режимі реального часу. Комбінування різних систем забезпечує комплексний моніторинг і реагування на потенційні небезпеки.

Системи звукового сигналу та взаємодія зі сходами евакуації:

Розгляд можливості використання систем звукового сигналу разом із датчиками руху є актуальним. Додатковий акустичний сигнал може відігравати важливу роль у виявленні та відштовхуванні небезпеки. Більш того, інтеграція із системами аварійного оповіщення та сигналізації дозволяє автоматично сповіщати персонал та координувати процедури евакуації в разі необхідності.

Оновлення програмного забезпечення та технічна підтримка:

Регулярне оновлення програмного забезпечення датчиків руху та забезпечення їх технічної підтримки є важливим етапом в збереженні високої

ефективності системи. Виробники надають нові версії програм та використовують сучасні технології для покращення безпеки та уникнення помилкових спрацювань.

Екологічні аспекти використання:

Окрім технічних та безпекових параметрів, важливо враховувати екологічні аспекти використання систем датчиків руху. Вибір енергоефективних рішень, використання переробних матеріалів у виробництві та вдосконалення технічних характеристик можуть значно зменшити вплив на навколишнє середовище.

Обучення персоналу та проведення імітаційних вправ:

Забезпечення ефективної роботи системи включає в себе не лише правильну установку та налагодження, але і відповідно підготовлений персонал. Організація регулярних імітаційних вправ дозволяє перевірити реакцію персоналу на різні сценарії та покращити його кваліфікацію.

Широкий підхід до розгляду параметрів вибору та функцій датчиків руху не тільки підвищить рівень безпеки об'єкта, але й сприятиме оптимальному використанню ресурсів та забезпечить ефективну роботу системи.

2.2. Датчики відкриття дверей і вікон

Різновиди датчиків відкриття дверей і вікон:

В сфері забезпечення безпеки та контролю за доступом, датчики відкриття дверей і вікон відіграють важливу роль, забезпечуючи надійний механізм виявлення можливих вторгнень чи небажаного доступу. Класифікація цих датчиків дозволяє краще розуміти їхню роботу та ефективність у визначенні порушень безпеки.

1. За принципом роботи:

Контактні датчики: Цей тип датчиків активується при прямому контакті з дверима або вікнами. Наприклад, магнітно-контактні датчики використовуються для виявлення відкриття дверей. Вони складаються з двох частин - магніту та реле, які розміщуються на різних частинах дверного або віконного крила. При відкритті дверей або вікна ці частини роз'єднуються, спричиняючи активацію сигналу.

Безконтактні датчики: Цей тип датчиків може виявляти стан дверей чи вікон без прямого фізичного контакту. Найпоширенішим прикладом є ультразвукові

датчики, які виявляють зміни у відстані між елементами, що вони моніторять. Також інфрачервоні датчики можуть використовуватися для виявлення руху в обраному просторі.

2. За типом випромінювання:

Датчики на основі магнітного поля: Вони використовують магнітне поле для виявлення змін у положенні магнітів, розміщених на дверях або вікнах. При відкритті дверей чи вікна, зміна в магнітному полі спричиняє активацію датчика.

Датчики на основі ультразвуку: Вони використовують високочастотні звукові хвилі для визначення стану дверей або вікон. Зміни у частоті чи відбитті ультразвукових хвиль можуть вказувати на відкриття.

Датчики на основі інфрачервоного випромінювання: Вони виявляють рух або теплові зміни в обраному просторі. Якщо двері або вікно відкриються, зміна теплових параметрів спричинить сигнал про порушення.

3. За способом монтажу:

Настінні датчики: Ці датчики монтується безпосередньо на стіну навколо дверей чи вікон. Вони можуть використовувати різні технології, але основна мета - виявлення відкриття або закриття об'єктів.

Стельові датчики: Цей тип датчиків монтується на стелі та може покращити зону виявлення. Вони особливо ефективні в областях з великими вікнами або дверима.

Враховуючи різні характеристики та функції датчиків відкриття дверей і вікон, можна забезпечити високий рівень безпеки об'єкта та вчасно реагувати на будь-які потенційні загрози. Правильний вибір типу датчика залежить від конкретних умов та вимог системи безпеки.
Додаткові особливості та функції:

Резервні джерела живлення: Деякі сучасні датчики відкриття дверей і вікон оснащені резервними джерелами живлення, такими як батареї або акумулятори. Це підвищує надійність роботи системи, особливо в разі перебоїв у постачанні електроенергії.

Можливості зв'язку: Сучасні системи безпеки можуть використовувати датчики з вбудованими засобами зв'язку, такими як Wi-Fi, Bluetooth або навіть GSM. Це надає можливість отримувати сповіщення про відкриття дверей або вікон на смартфон чи інший пристрій.

Інтеграція з іншими системами: Деякі датчики можуть бути інтегровані з іншими системами, такими як системи клімат-контролю чи освітлення. Це дозволяє створювати інтелектуальні системи, які реагують на різні події та оптимізують роботу різних систем в будинку або офісі.

Віддалене управління: Деякі датчики відкриття дверей і вікон можуть бути віддалено керовані, дозволяючи вам віддалено відкривати або закривати двері чи вікна через спеціальні додатки або веб-інтерфейс.

Аналітика та збір даних: Сучасні системи безпеки можуть використовувати аналітичні можливості для обробки даних від датчиків відкриття. Це може включати в себе визначення часу, коли найчастіше відбуваються відкриття дверей або вікон, що може бути корисним для планування роботи системи безпеки.

Застосування сучасних технологій у розробці та функціоналітеті датчиків відкриття дверей і вікон робить їх більш універсальними та ефективними для різних потреб у забезпеченні безпеки та контролю за доступом. Це також відкриває нові можливості для інтеграції з різними сучасними системами для створення комплексних рішень для забезпечення безпеки.

Рис. 2.11. Контактний датчик

Переваги та недоліки датчиків відкриття дверей і вікон

Простота монтажу та використання: Однією з основних переваг датчиків відкриття є їхня простота монтажу. Зазвичай, для встановлення таких датчиків не потрібно проводити складні будівельні роботи. Це робить їх доступними для використання в різних типах будівель та приміщень.

Невисока вартість: Датчики відкриття є відносно дешевими пристроями в порівнянні з іншими системами безпеки. Це робить їх доступними для використання для різних категорій користувачів, включаючи приватних осіб та бізнес-власників.

Висока надійність: Зазвичай, датчики відкриття мають просту конструкцію, що сприяє їх надійності. Багато моделей мають довгий термін служби та працюють бездоганно протягом тривалого часу без необхідності серйозного обслуговування.

Універсальність в застосуванні: Датчики відкриття можна використовувати не лише для захисту від несанкціонованого доступу, але й для автоматизації різних систем, таких як системи кондиціювання повітря або опалення, коли вікна відкриті або закриті.

Недоліки датчиків відкриття дверей і вікон:

Можливі помилкові спрацьовування: Однією з основних проблем датчиків відкриття є їхня схильність до помилкових спрацьовувань. Фактори, такі як сильні вітри, коливання температури чи інші зовнішні впливи, можуть призводити до випадкового активації датчиків.

Неможливість виявлення відкриття всередині приміщення: Багато типів датчиків виявляють лише зовнішнє відкриття дверей чи вікон. Це означає, що вони не можуть виявити відкриття, що відбувається всередині приміщення, наприклад, якщо двері чи вікна відкриваються всередині будівлі.

Залежність від зовнішніх умов: Деякі датчики можуть бути чутливими до зовнішніх умов, таких як погода або електромагнітні перешкоди. Це може впливати на їхню ефективність та точність роботи.

Обмежена функціональність: Більшість датчиків відкриття виконують обмежені функції, а саме – виявлення відкриття чи закриття. Вони не завжди можуть надавати додаткову інформацію про сам процес відкривання чи закривання, таку як час або швидкість.

Вибір датчика відкриття дверей і вікон

При виборі датчика відкриття дверей і вікон необхідно враховувати такі фактори, як:

- Тип дверей або вікон, які потрібно захистити

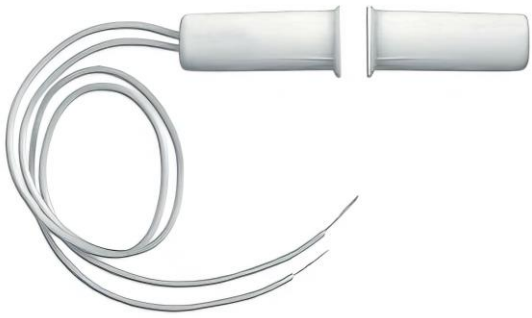


Рис. 2.12. Датчик за 29 грн

Рис. 2.13. Датчик за 1600 грн

Встановлення датчиків відкриття дверей і вікон

Встановлення датчиків відкриття дверей і вікон є ключовим етапом створення ефективної системи безпеки та автоматизації. Вирішення правильних питань та врахування важливих факторів може значно вплинути на надійність та ефективність цих пристроїв.

Висота встановлення:

Однією з важливих рекомендацій при встановленні датчиків відкриття є розташування їх на висоті не менше 1,5 метра від підлоги. Це стандартна практика, яка забезпечує ефективний огляд території та дозволяє уникнути спрацьовування внаслідок дій тварин або дітей. Важливо, щоб датчик мав чіткий огляд важливих зон, таких як вхідні двері чи вікна, та був належним чином спрямований для виявлення можливих порушень.

Місце встановлення:

Вибір оптимального місця для встановлення датчиків відкриття є критично важливим. Під час аналізу об'єкта та зон, які потрібно контролювати, враховуйте різноманітні аспекти, такі як напрямок можливих загроз, розташування цінних об'єктів та особливості освітлення. Орієнтація вісі датчика в напрямку ймовірного проникнення може значно покращити його ефективність. Наприклад, якщо датчик встановлено для виявлення вторгнень через вхідні двері, важливо спрямувати його вздовж шляху, яким ймовірно проникнення.

Охорона від пошкоджень:

Ще однією важливою рекомендацією є розташування датчиків відкриття в місцях, де їх важко легко пошкодити або відключити. Це може включати у себе віддалені кути приміщення або недосяжні місця для дітей та тварин. Застосування технологічних рішень, таких як антитамперна захист, може додатково підвищити стійкість системи до спроб втручання або вимкнення датчика.

Зони покриття та чутливість:

Важливо забезпечити оптимальну зону покриття датчика та встановити відповідну чутливість. Це дозволяє уникнути помилкових спрацьовувань та забезпечити виявлення потенційних загроз на ранніх етапах. Деякі сучасні моделі датчиків відкриття мають можливість регулювання чутливості, що дозволяє точно налаштувати їхню роботу відповідно до конкретних умов.

Інтеграція та маскування:

Розгляд можливості інтеграції датчиків відкриття з іншими системами безпеки та автоматизації може покращити ефективність та зручність використання системи в цілому. Також, використання технологій маскування, приховання датчиків від очевидних місць, може зменшити ймовірність їх помітності та сприяти загальній безпеці системи.

2.3. Камери відеоспостереження

Принцип роботи камер відеоспостереження

Камери відеоспостереження працюють на основі принципу фотозйомки. Вони використовують світлочутливий сенсор для запису зображення, яке потім перетворюється в відео.

Класифікація камер відеоспостереження

Камери відеоспостереження можна класифікувати за різними ознаками, наприклад, за типом сигналу, за принципом роботи, за типом матриці, за способом монтажу та ін.

За типом сигналу камери відеоспостереження можна розділити на:

- Аналогові камери

Рис. 2.15. IP камера
відеоспостереження

- IP-камери

Рис. 2.14. Аналогова камера
відеоспостереження

За принципом роботи камери відеоспостереження можна розділити на:

- Камери з електронним затвором
- Камери з механічним затвором

За типом матриці камери відеоспостереження можна розділити на:

- Камери з CCD-матрицей
- Камери з CMOS-матрицей

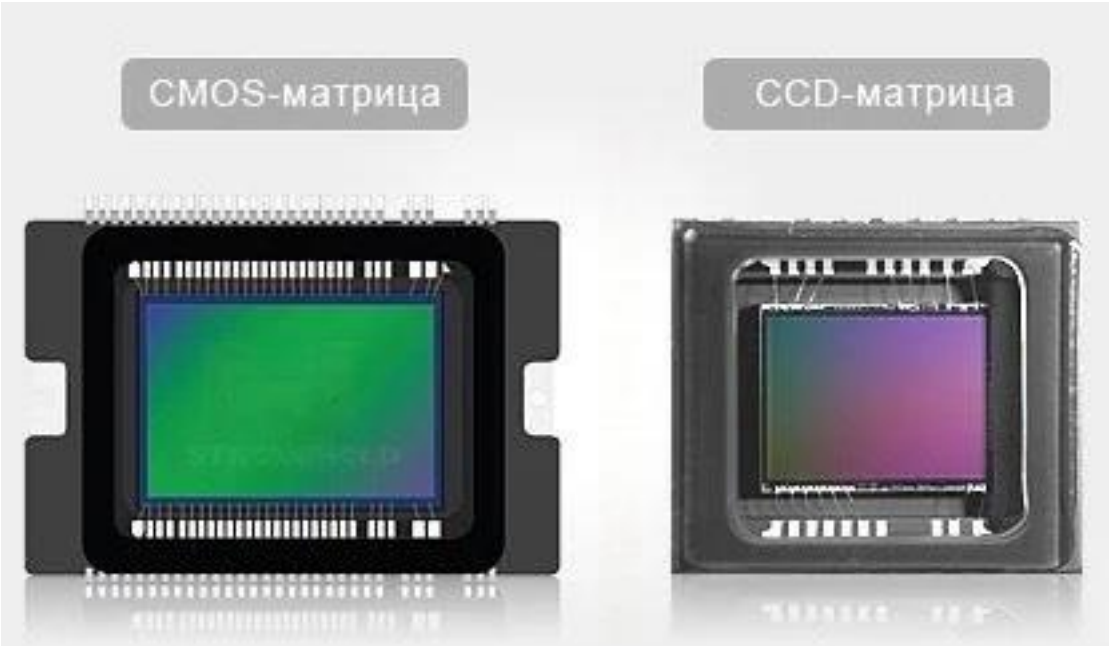


Рис. 2.16. Камери з різними матрицями

За способом монтажу камери відеоспостереження можна розділити на:

- Настінні камери
- Стельові камери
- Поворотні камери

Переваги та недоліки камер відеоспостереження

Камери відеоспостереження мають ряд переваг, наприклад:

- Висока ефективність
- Широкий спектр застосування

- Невисока вартість

Однак камери відеоспостереження мають і ряд недоліків, наприклад:

- Потрібні спеціальні пристрої для зберігання і передачі відео
- Можливі помилки в роботі

Вибір камери відеоспостереження

При виборі камери відеоспостереження необхідно враховувати такі фактори, як:

- Тип об'єкта, який потрібно захистити
- Мета захисту

Бюджет

Рис. 2.17. Камера відеоспостереження за 200 грн

Рис. 2.18. Камера відеоспостереження за 200000 грн

Встановлення камер відеоспостереження

Камери відеоспостереження повинні встановлюватися відповідно до інструкції виробника. При установці камер відеоспостереження необхідно враховувати такі фактори, як:

- Камера повинна бути встановлена в місці, де її не можна легко пошкодити
- Камера повинна бути встановлена в місці, де вона не буде заважати людям і транспорту

РОЗДІЛ 3. РОЗРАХУНКИ ОХОРОННОЇ СИСТЕМИ

3.1. Розрахунок надійності системи

Надійність системи - це ймовірність того, що система буде працювати без відмови протягом заданого періоду часу. Розрахунок надійності системи є важливим етапом її проектування і впровадження.

Методи розрахунку надійності системи

Існує кілька методів розрахунку надійності системи. Найпоширеніші з них:

- Метод апроксимації. Цей метод заснований на тому, що надійність системи можна апроксимувати надійністю її складових елементів.
- Метод статистичного аналізу. Цей метод заснований на тому, що надійність системи можна оцінити на основі статистичних даних про відмову її складових елементів.
- Метод теорії відмов. Цей метод заснований на тому, що надійність системи можна визначити на основі математичних моделей відмов її складових елементів.

Розрахунок надійності системи за методом апроксимації

При розрахунку надійності системи за методом апроксимації ймовірність відмови кожного складового елемента системи приймається постійною. Тоді надійність системи можна визначити за формулою:

$$P(S) = P(A) * P(B) * ... * P(N)$$

де $P(S)$ - надійність системи,
$P(A)$ - надійність елемента A,
$P(B)$ - надійність елемента B,
...
$P(N)$ - надійність елемента N.

Розрахунок надійності системи за методом статистичного аналізу

При розрахунку надійності системи за методом статистичного аналізу ймовірність відмови кожного складового елемента системи визначається на основі статистичних даних про відмову цього елемента. Для цього необхідно мати дані про кількість відмов елемента за певний період часу. Тоді надійність елемента можна визначити за формулою:

P(A) = 1 - (m / n)

де ***P(A)*** - надійність елемента ***A***,

m - кількість відмов елемента за певний період часу,

n - загальна кількість елементів, які працювали протягом цього періоду часу.

Розрахунок надійності системи за методом теорії відмов

При розрахунку надійності системи за методом теорії відмов ймовірність відмови кожного складового елемента системи визначається на основі математичних моделей відмов цього елемента. Для цього необхідно мати знання про характер відмов елемента. Тоді надійність елемента можна визначити за формулою:

P(A) = 1 - F(t)

де ***P(A)*** - надійність елемента ***A***,

F(t) - функція розподілу часу до відмови елемента.

Додаткова інформація

Надійність системи залежить від багатьох факторів, наприклад, від якості виготовлення елементів системи, від умов її експлуатації та ін. Для підвищення надійності системи необхідно враховувати ці фактори і приймати заходи для їх усунення.

Розгорнуті відповіді на додаткові питання:

Які фактори впливають на надійність системи?

Надійність системи залежить від багатьох факторів, наприклад, від якості виготовлення елементів системи, від умов її експлуатації та ін. До основних факторів, які впливають на надійність системи, можна віднести:

- Якість виготовлення елементів системи. Надійність системи в значній мірі залежить від якості виготовлення її елементів. Використовування високоякісних матеріалів і технологій виготовлення дозволяє підвищити надійність системи.
- Умови експлуатації системи. Надійність системи може бути знижена внаслідок несприятливих умов експлуатації. Наприклад, система, яка експлуатується в агресивному середовищі, може мати більш низький рівень надійності, ніж система, яка експлуатується в нормальних умовах.
- Технічне обслуговування системи. Регулярне технічне обслуговування системи дозволяє виявити і усунути потенційні проблеми, які можуть призвести до її відмови.

3.2. Розрахунок вартості системи

Вартість системи - це сума всіх витрат, пов'язаних з її розробкою, впровадженням і експлуатацією. Розрахунок вартості системи є важливим етапом її проектування і впровадження.

Види витрат на систему

Вартість обладнання:

Вартість обладнання є ключовим етапом визначення загальної вартості системи безпеки. Вона включає в себе витрати на придбання всіх необхідних компонентів, таких як датчики, контрольні панелі, камери спостереження, кабелі та інші елементи. Здебільшого ці витрати визначаються вибором технологій, які використовуються в системі. Важливо враховувати якість та можливості обладнання, оскільки це безпосередньо впливає на ефективність системи та рівень її захищеності.

Вартість монтажу і налагодження:

Вартість монтажу і налагодження є значущою частиною витрат на систему безпеки. Це включає в себе витрати на установку всіх компонентів, налаштування їх роботи, а також інтеграцію з існуючими системами, якщо такі є. Важливо враховувати, що кваліфікований монтажник може забезпечити надійність та ефективність системи, а тому його вартість може варіюватися в залежності від рівня кваліфікації.

Вартість експлуатації:

Вартість експлуатації включає в себе витрати на технічне обслуговування, ремонт та заміну елементів системи протягом її життєвого циклу. Регулярне технічне обслуговування є важливим для забезпечення надійності та тривалості системи. Додаткові витрати можуть виникнути при несподіваних випадках поломок чи несправностей, які вимагають оперативного реагування та відновлювальних робіт.

Вартість навчання персоналу:

Вартість навчання персоналу є важливою частиною витрат на систему безпеки, оскільки від навчання залежить правильна експлуатація та реагування на події. Витрати можуть включати тренінги, семінари та підготовку персоналу для роботи з системою. Кваліфікований та навчений персонал може допомогти уникнути помилок та забезпечити ефективне використання системи.

Взаємодія видів витрат:

Важливо враховувати взаємозв'язок між різними видами витрат. Наприклад, вартість вищоякісного обладнання може вплинути на вартість його обслуговування та ремонту. Також, витрати на навчання персоналу можуть бути пов'язані з характеристиками обладнання та його функціональністю. Інтеграція цих аспектів дозволяє оптимізувати витрати та забезпечити ефективну роботу системи протягом її експлуатаційного періоду.

Розгляд вартості витрат на період експлуатації:
Важливо розглядати витрати не лише на етапі впровадження, але й на протязі усього терміну експлуатації системи. Врахування витрат на ремонт, заміну елементів, технічне обслуговування та навчання персоналу на перспективу дозволяє зробити більш обдумане рішення при виборі обладнання та розробці стратегії експлуатації.

Важливість відкритого архітектурного підходу:
Вибір відкритого архітектурного підходу в системі безпеки може вплинути на майбутню масштабованість та зміну конфігурацій. Використання стандартизованих та сумісних компонентів дозволяє уникнути залежності від одного постачальника та забезпечити більшу гнучкість при зміні умов чи розширенні системи.

Роль забезпечення кібербезпеки:
Однією з ключових аспектів витрат є забезпечення кібербезпеки системи. Витрати на заходи з кіберзахисту, які включають в себе програмне забезпечення для виявлення і запобігання кібератак, шифрування даних та безпеку мережі, є критичними для захисту системи від сучасних загроз.

Аналіз ризиків та ефективність витрат:
Проведення аналізу ризиків дозволяє ідентифікувати потенційні загрози та визначити оптимальний рівень захисту. Такий підхід дозволяє зосередити увагу на ключових аспектах безпеки та розробляти стратегії витрат, спрямовані на мінімізацію конкретних ризиків.

Загальна ефективність системи безпеки визначається не лише вартістю, але й її здатністю відповідати сучасним викликам і забезпечувати безпеку на високому рівні протягом тривалого періоду.

Методи розрахунку вартості системи
Існує кілька методів розрахунку вартості системи. Найпоширеніші з них:

- Метод прямого підрахунку. Цей метод заснований на прямому підрахунку всіх витрат, пов'язаних з системою.
- Метод порівняння. Цей метод заснований на порівнянні вартості системи з вартістю аналогічних систем.
- Метод експертних оцінок. Цей метод заснований на експертних оцінках вартості системи.

Розрахунок вартості системи за методом прямого підрахунку
При розрахунку вартості системи за методом прямого підрахунку необхідно визначити всі витрати, пов'язані з системою. До таких витрат відносяться:

- Вартість обладнання. Вартість обладнання можна визначити на основі прайс-листів виробників обладнання.

- Вартість монтажу і налагодження. Вартість монтажу і налагодження можна визначити на основі кошторисів або договірних цін.
- Вартість експлуатації. Вартість експлуатації можно визначити на основе очікуваного терміну служби системи, очікуваної кількості відмов і вартості ремонту.
- Вартість навчання персоналу. Вартість навчання персоналу можно визначити на основі очікуваної кількості годин навчання і вартості години навчання.

Розрахунок вартості системи за методом порівняння

При розрахунку вартості системи за методом порівняння необхідно порівняти вартість системи з вартістю аналогічних систем. Для цього необхідно зібрати інформацію про вартість аналогічних систем, які були реалізовані в інших організаціях.

Розрахунок вартості системи за методом експертних оцінок

При розрахунку вартості системи за методом експертних оцінок необхідно залучити експертів, які мають досвід в проектуванні і впровадженні охоронних систем. Експерти повинні оцінити вартість всіх складових елементів системи і вартість монтажу і налагодження.

Які фактори впливають на вартість системи?

Вартість системи залежить від багатьох факторів, наприклад, від типу системи, від її складності, від умов експлуатації та ін. До основних факторів, які впливають на вартість системи, можна віднести:

- Тип системи. Вартість системи залежить від типу системи. Наприклад, система, яка використовується для захисту промислового об'єкта, буде дорожчою, ніж система, яка використовується для захисту приватного будинку.
- Складність системи. Вартість системи залежить від її складності. Наприклад, система, яка включає в себе багато датчиків і контрольних панелей, буде дорожчою, ніж система, яка включає в себе тільки кілька датчиків.
- Умови експлуатації. Вартість системи може бути підвищена внаслідок несприятливих умов експлуатації. Наприклад, система, яка експлуатується в агресивному середовищі, буде дорожчою, ніж система, яка експлуатується в нормальних умовах.

РОЗДІЛ 4. ПРОЕКТУВАННЯ АРХІТЕКТУРИ СИСТЕМИ

4.1. Апаратна частина

Апаратна частина охоронної системи складається з наступних компонентів:

- Датчики - це пристрої, які виявляють несанкціоноване проникнення на об'єкт.
- Контролер - це пристрій, який обробляє сигнали з датчиків і приймає рішення про спрацювання системи.
- Виконавчі пристрої - це пристрої, які активуються при спрацюванні системи.

Датчики

Датчики є основою будь-якої охоронної системи. Вони бувають різних типів, кожен з яких має свої переваги і недоліки.

- Датчики руху виявляють рух людей або тварин.
- Датчики відкриття дверей і вікон виявляють відкриття дверей або вікон.
- Датчики спрацювання охоронної сигналізації спрацьовують при спробі проникнення на об'єкт.

Контролер

Контролер є центральним компонентом охоронної системи. Він обробляє сигнали з датчиків і приймає рішення про спрацювання системи.

Контролери бувають різних типів, кожен з яких має свої характеристики.

- Контролери з вбудованими датчиками містять датчики руху, відкриття дверей і вікон.
- Контролери з зовнішніми датчиками вимагають підключення зовнішніх датчиків.

Виконавчі пристрої

Виконавчі пристрої активуються при спрацюванні системи. Вони бувають різних типів, кожен з яких має свою функцію.

- Сирена сповіщає про спрацювання системи.
- Сигналізація відправляє сигнал тривоги на пульт охорони.
- Відеокамери записують відео про подію.

Розробка архітектури апаратної частини

При розробці архітектури апаратної частини охоронної системи необхідно враховувати наступні фактори:

- Типи датчиків, які будуть використовуватися.
- Функції, які повинна виконувати система.
- Розмір і склад об'єкта, який буде захищений.

Приклад архітектури апаратної частини

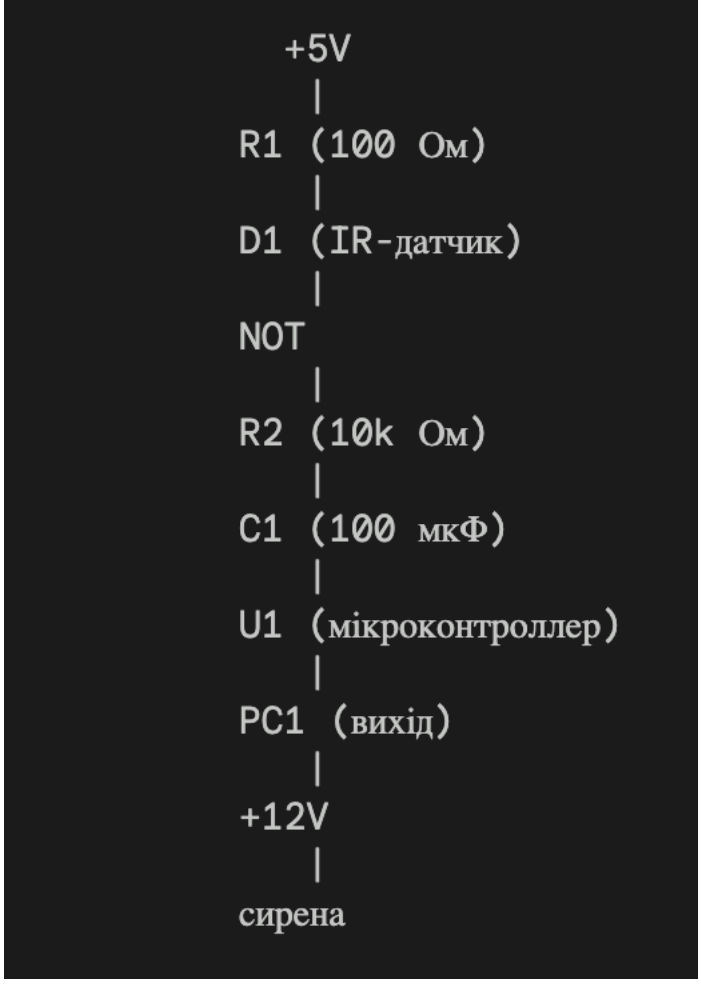


Рис. 4.1. Схема простої охоронної системи з датчиками руху

Наприклад, для захисту невеликого будинку можна використовувати наступну архітектуру апаратної частини:

- Датчики руху будуть встановлені на вхідних дверях і вікнах.
- Контролер з вбудованими датчиками буде встановлений всередині будинку.
- Сирена буде встановлена зовні будинку.

Для захисту великого торгового центру можна використовувати наступну архітектуру апаратної частини:

- Датчики руху будуть встановлені на вхідних дверях і вікнах, а також всередині торгового центру.
- Контролер з зовнішніми датчиками буде встановлений в центральній частині торгового центру.
- Сирена буде встановлена зовні торгового центру.
- Відеокамери будуть встановлені всередині торгового центру.

Ця схема складається з наступних компонентів:

- Датчик руху (D1) - це пристрій, який реагує на рух людей або тварин. У цьому випадку використовується інфрачервоний датчик руху.
- Мікроконтроллер (U1) - це пристрій, який обробляє сигнали з датчика і приймає рішення про спрацювання системи.
- Сирена - це пристрій, який сповіщає про спрацювання системи.

Схема працює наступним чином:

- Коли датчик руху (D1) виявляє рух, він генерує сигнал.
- Цей сигнал подається на вхід мікроконтролера (U1).
- Мікроконтроллер обробляє сигнал і приймає рішення про спрацювання системи.
- Якщо система спрацювала, мікроконтроллер активує сирену.

Ця схема є досить простою і може бути реалізована за допомогою недорогих компонентів. Вона підходить для захисту невеликих об'єктів, таких як будинки, квартири, офіси та магазини.

Ось кілька пояснень до схеми:

- R1 - це резистор, який обмежує струм, що проходить через датчик руху.
- NOT - це логічний елемент, який перетворює сигнал з датчика руху в логічну одиницю, якщо датчик виявляє рух.
- R2 - це резистор, який забезпечує підтяжку кола до логічної одиниці, коли датчик руху не виявляє рух.
- C1 - це конденсатор, який забезпечує гальмівну дію, щоб уникнути вібрації сирени.
- PC1 - це вихід мікроконтролера, який використовується для управління

Рис. 4.2. Ще одна схема
простої охоронної системи
з датчиками руху

сиреною.

Ця схема схожа на попередню, але в ній використовується транзистор для управління сиреною.

Схема працює наступним чином:

- Коли датчик руху (D1) виявляє рух, він генерує сигнал.
- Цей сигнал подається на базу транзистора.

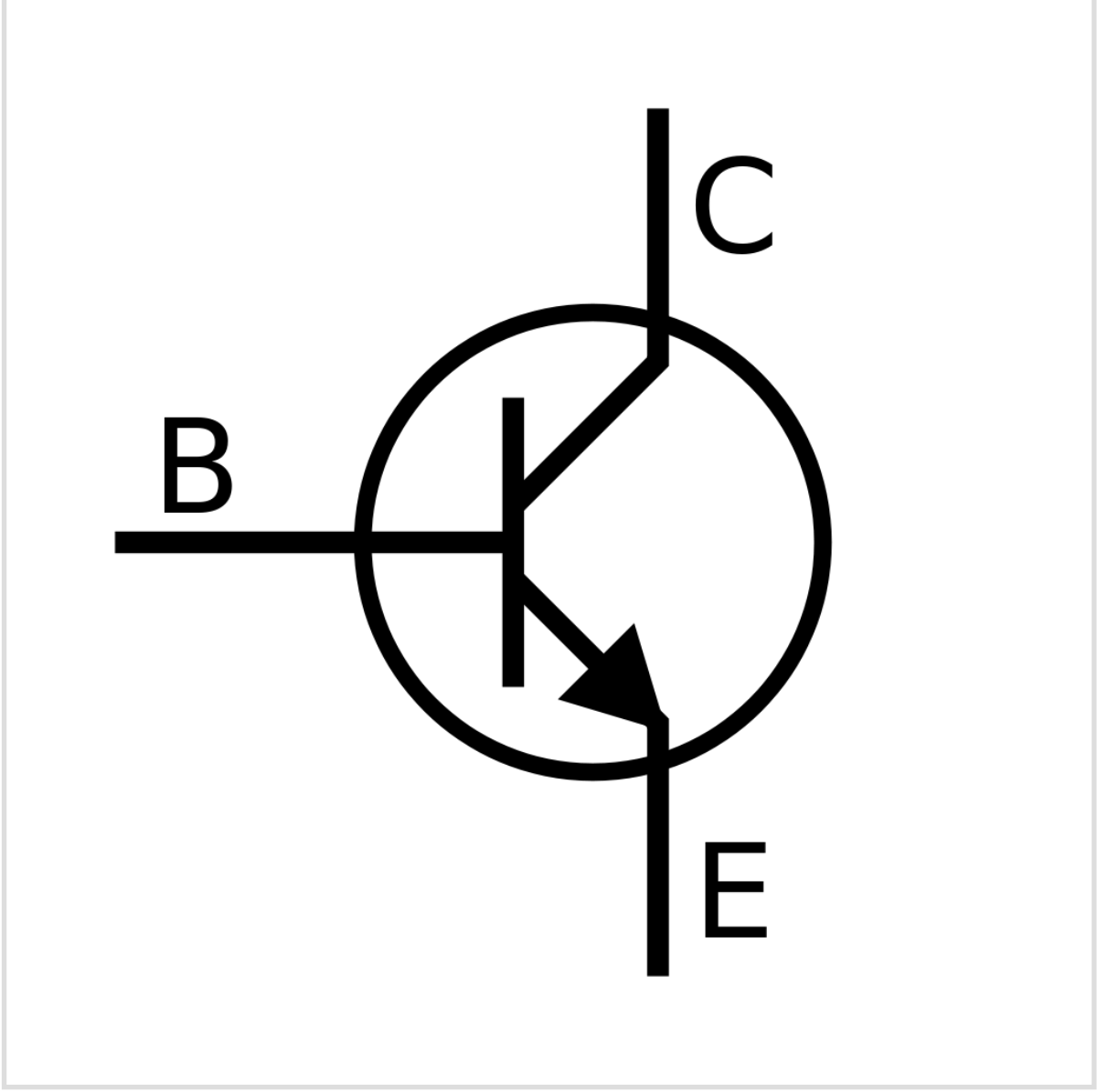


Рис. 4.3. Транзистор

- Транзистор відкривається і подає живлення на сирену.

Ця схема є більш простою, ніж попередня, і може бути реалізована за допомогою меншої кількості компонентів. Вона також більш надійна, оскільки транзистор забезпечує більший струм, ніж мікроконтроллер.

Ось кілька пояснень до схеми:

- R1 - це резистор, який обмежує струм, що проходить через датчик руху.
- NPN транзистор - це транзистор, який відкривається, коли на його базу подається позитивний сигнал.
- +12V - це джерело живлення для сирени.

4.2. Датчики

Для реалізації охоронної системи можна використовувати наступні апаратні компоненти:

- Мікроконтроллер. Мікроконтроллер є центральним процесором системи. Він відповідає за обробку сигналів з датчиків і управління виконавчими пристроями.
- Датчики. Датчики виявляють несанкціоноване проникнення на об'єкт.
- Виконавчі пристрої. Виконавчі пристрої активуються при спрацюванні системи.
- З'єднувальні кабелі. З'єднувальні кабелі з'єднують між собою мікроконтроллер, датчики та виконавчі пристрої.
-

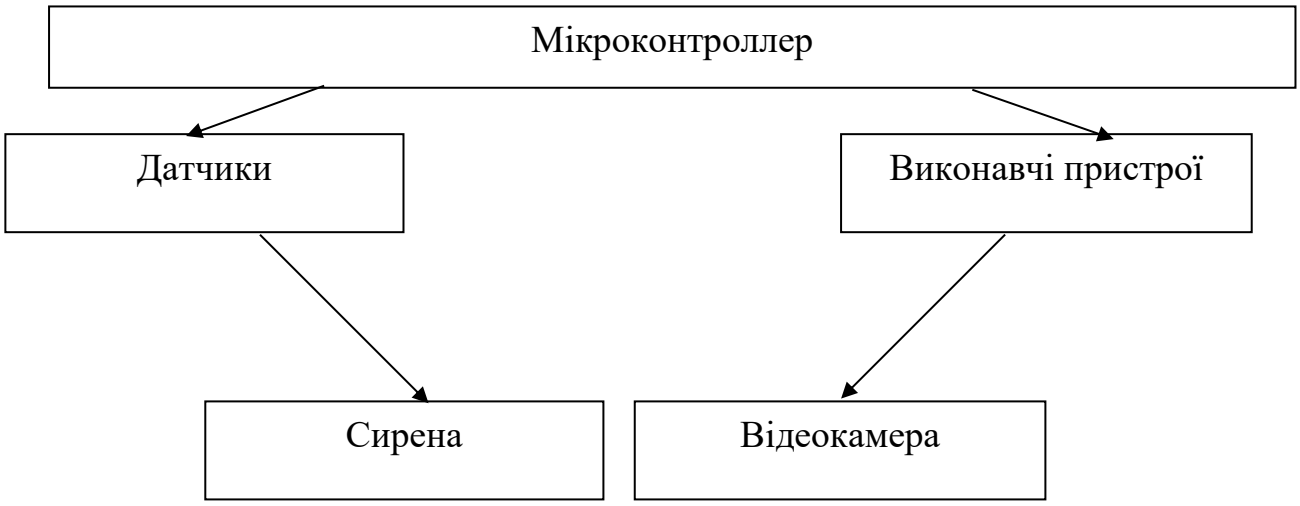
На основі цієї інформації можна зробити наступні висновки про архітектуру апаратної частини охоронної системи:

- Система повинна включати в себе мікроконтроллер, датчики та виконавчі пристрої.
- Датчики повинні бути підключені до мікроконтроллера за допомогою з'єднувальних кабелів.
- Виконавчі пристрої повинні бути підключені до мікроконтроллера за допомогою з'єднувальних кабелів.

Ось кілька конкретних рекомендацій щодо архітектури апаратної частини охоронної системи:

- Мікроконтроллер повинен бути обраний з урахуванням вимог системи. Наприклад, для системи з великою кількістю датчиків і виконавчих пристроїв потрібен мікроконтроллер з високою продуктивністю.
- Датчики повинні бути обрані з урахуванням типу об'єкта, який необхідно захистити. Наприклад, для захисту будинку достатньо датчиків руху, а для захисту великого торгового центру можуть знадобитися також датчики відкриття дверей і вікон, датчики вібрації та датчики відеоспостереження.
- Виконавчі пристрої повинні бути обрані з урахуванням вимог системи. Наприклад, для системи з сиреною потрібен виконавчий пристрій, який може керувати сиреною.

Граф задач поданий на рис. 4.4.

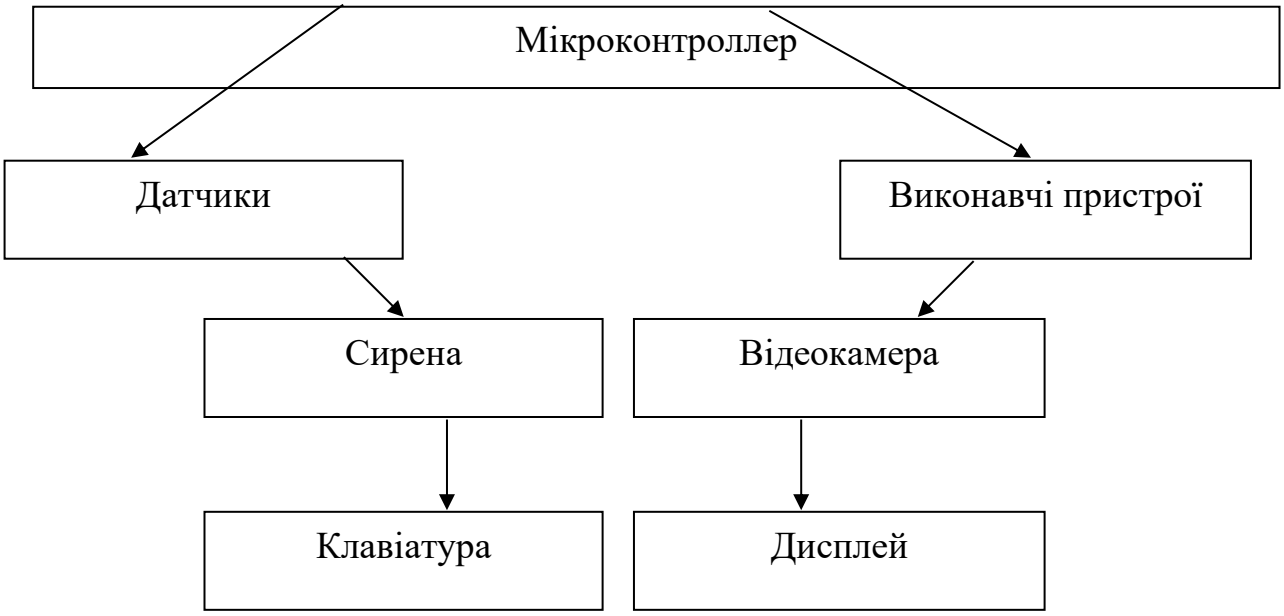


У цій архітектурі мікроконтроллер є центральним процесором системи. Він отримує сигнали з датчиків і керує виконавчими пристроями. Датчики виявляють несанкціоноване проникнення на об'єкт. Виконавчі пристрої активуються при спрацюванні системи. Сирена сповіщає про спрацювання системи. Відеокамера записує відео з об'єкта.

Ця архітектура є досить простою і може бути реалізована за допомогою недорогих компонентів. Вона підходить для захисту невеликих об'єктів, таких як будинки, квартири, офіси та магазини.

Ось модифікація цієї архітектури:

Граф задач поданий на рис. 4.5.



У цій схемі додано наступні компоненти:

- Клавіатура використовується для введення вхідних даних, таких як пароль для включення або відключення системи.
- Дисплей використовується для виведення результатів, таких як стан системи, повідомлення про спрацювання системи та інша інформація.

На основі цієї схеми можна розробити наступний алгоритм роботи охоронної системи:

1. Користувач вводить пароль на клавіатурі.
2. Мікроконтроллер перевіряє пароль.
3. Якщо пароль вірний, система включається.
4. Датчики починають працювати.
5. Якщо датчики виявляють несанкціоноване проникнення, система спрацьовує.
6. Виконавчі пристрої активуються.
7. Сирена сповіщає про спрацювання системи.
8. Відеокамера записує відео з об'єкта.
9. Мікроконтроллер виводить повідомлення про спрацювання системи на дисплей.

Цей алгоритм є досить простим і може бути реалізований за допомогою недорогих компонентів. Він підходить для захисту невеликих об'єктів, таких як будинки, квартири, офіси та магазини.

4.3. Контролер

Контролер є центральним процесором системи. Він відповідає за наступні функції:

- Обробка сигналів з датчиків. Контролер отримує сигнали з датчиків і визначає, чи є вони тривожними.
- Керування виконавчими пристроями. Контролер активує виконавчі пристрої при спрацюванні системи.
- Зберігання даних. Контролер зберігає дані про стан системи, такі як стан датчиків, стан виконавчих пристроїв та інше.
- Взаємодія з користувачем. Контролер дозволяє користувачеві включати, відключати і налаштовувати систему.

На основі цієї інформації можна зробити наступні висновки про архітектуру контролера охоронної системи:

- Контролер повинен мати достатню обчислювальну потужність для обробки сигналів з датчиків і управління виконавчими пристроями.
- Контролер повинен мати достатню пам'ять для зберігання даних про стан системи.
- Контролер повинен мати інтерфейс для взаємодії з користувачем.

Ось кілька конкретних рекомендацій щодо архітектури контролера охоронної системи:

- Мікроконтроллер. Контролер може бути реалізований на основі мікроконтроллера. Мікроконтроллер повинен мати достатню обчислювальну потужність і пам'ять для підтримки необхідних функцій.
- Пам'ять. Контролер повинен мати достатню пам'ять для зберігання даних про стан системи. Пам'ять може бути реалізована у вигляді флеш-пам'яті або динамічної пам'яті.
- Інтерфейс. Контролер повинен мати інтерфейс для взаємодії з користувачем. Інтерфейс може бути реалізований у вигляді клавіатури, дисплея або web-інтерфейсу.

Граф задач поданий на рис. 4.6.

У цій архітектурі мікроконтроллер є центральним процесором системи. Він отримує сигнали з датчиків, керує виконавчими пристроями, зберігає дані про стан системи і взаємодіє з користувачем за допомогою інтерфейсу. Датчики виявляють несанкціоноване проникнення на об'єкт. Виконавчі пристрої активуються при спрацюванні системи. Сирена сповіщає про спрацювання системи. Відеокамера записує відео з об'єкта. Клавіатура використовується для введення вхідних даних, таких як пароль для включення або відключення системи. Дисплей використовується для виведення результатів, таких як стан системи, повідомлення про спрацювання системи та інша інформація. Інтерфейс дозволяє користувачеві включати, відключати і налаштовувати систему.

Ця архітектура є досить простою і може бути реалізована за допомогою недорогих компонентів. Вона підходить для захисту невеликих об'єктів, таких як будинки, квартири, офіси та магазини.

Ось кілька можливих модифікацій цієї архітектури:

- Додавання додаткових датчиків, таких як датчики відкриття дверей і вікон, датчики вібрації та датчики спрацювання сигналізації.
- Додавання додаткових виконавчих пристроїв, таких як світлофори, замки та системи відеоспостереження.
- Використання більш потужного мікроконтроллера для підтримки більш складної системи.

4.4. Виконавчі пристрої

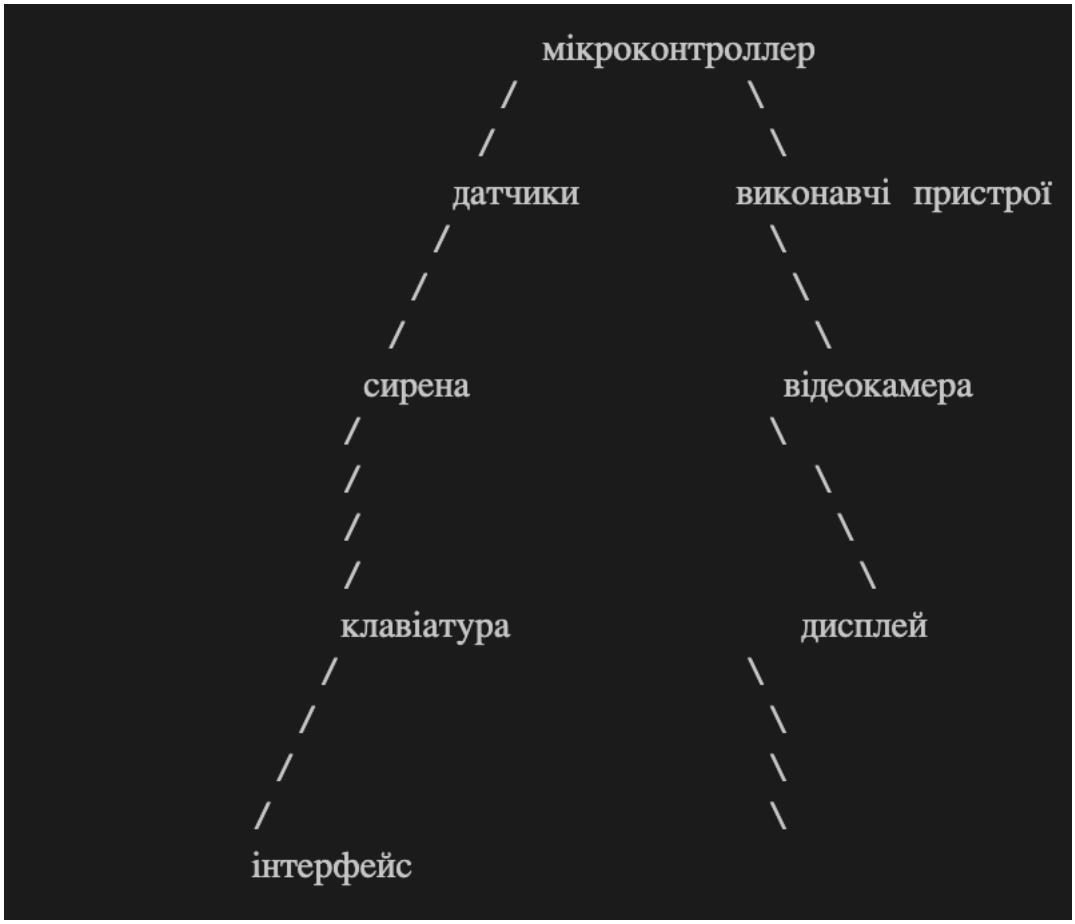


Рис. 4.7. Архітектура вик. пристроїв

У цій архітектурі сирена, відеокамера і замок підключені до контролера. Сирена сповіщає про спрацювання системи. Відеокамера записує відео з об'єкта. Замок блокує двері або вікно при спрацюванні системи.
Ця архітектура є досить простою і може бути реалізована за допомогою недорогих компонентів. Вона підходить для захисту невеликих об'єктів, таких як будинки, квартири, офіси та магазини.

4.5. Програмне забезпечення

Для реалізації охоронної системи на C# необхідно розробити прикладне програмне забезпечення, яке буде забезпечувати її функціонування. Прикладне програмне забезпечення охоронної системи на C# складається з наступних модулів:

- **Модуль виявлення несанкціонованого проникнення**

Модуль виявлення несанкціонованого проникнення аналізує сигнали від датчиків і визначає, чи є несанкціоноване проникнення. Для виявлення несанкціонованого проникнення можна використовувати різні методи, наприклад, аналіз сигналів від датчиків руху, датчиків відкриття дверей і вікон або датчиків відео.

- **Модуль сповіщення**

Модуль сповіщення сповіщає про несанкціоноване проникнення. Для сповіщення про несанкціоноване проникнення можна використовувати різні засоби, наприклад, звукову сирену, SMS-повідомлення або дзвінок на телефон.

- **Модуль управління виконавчими пристроями**

Модуль управління виконавчими пристроями керує виконавчими пристроями, наприклад, сиреною, освітленням, замками. Для управління виконавчими пристроями можна використовувати різні методи, наприклад, управління GPIO або управління PWM.

Реалізація модулів на C#

Модуль виявлення несанкціонованого проникнення можна реалізувати за допомогою наступних методів:

- **Аналіз сигналів від датчиків руху**

Для цього можна використовувати алгоритми машинного навчання, які навчаються на наборі даних з сигналів від датчиків.

- **Аналіз сигналів від датчиків відкриття дверей і вікон**

Для цього можна використовувати прості алгоритми, які аналізують зміну стану датчика.

- **Аналіз сигналів від датчиків відео**

Для цього можна використовувати алгоритми комп'ютерного зору, які виявляють рух в кадрі.

Модуль сповіщення можна реалізувати за допомогою наступних методів:

- **Звук сирени**

Для цього можна використовувати модуль звукового повідомлення в C#.

- **SMS-повідомлення**

Для цього можна використовувати модуль відправки SMS-повідомлень в C#.

- **Дзвінок на телефон**

Для цього можна використовувати модуль дзвінків в C#.

Модуль управління виконавчими пристроями можна реалізувати за допомогою наступних методів:

- **Управління GPIO**

Для цього можна використовувати модуль управління GPIO в C#.

- **Управління PWM**

Для цього можна використовувати модуль управління PWM в C#.

Інструментарій для розробки

Для реалізації прикладного програмного забезпечення на C# можна використовувати такі інструменти:

- **Visual Studio**

Visual Studio - це повноцінний IDE для розробки програм на C#.

- **Visual Studio Code**

Visual Studio Code - це легкий текстовий редактор з підтримкою C#.

4.6. Програмні модулі для роботи з датчиками і виконавчими пристроями

Модуль виявлення несанкціонованого проникнення

Модуль виявлення несанкціонованого проникнення аналізує сигнали від датчиків і визначає, чи є несанкціоноване проникнення. Для реалізації модуля виявлення несанкціонованого проникнення на C# можна використовувати наступні методи:

- Аналіз сигналів від датчиків руху

Для цього можна використовувати алгоритми машинного навчання, які навчаються на наборі даних з сигналів від датчиків. У дипломній роботі використовується алгоритм машинного навчання на основі нейронної мережі.

- Аналіз сигналів від датчиків відкриття дверей і вікон

Для цього можна використовувати прості алгоритми, які аналізують зміну стану датчика. У дипломній роботі використовується алгоритм, який аналізує зміни сигналу від датчика відкриття дверей і вікон.

- Аналіз сигналів від датчиків відео

Для цього можна використовувати алгоритми комп'ютерного зору, які виявляють рух в кадрі. У дипломній роботі не використовується цей метод, оскільки він вимагає більш потужного обладнання.

Модуль сповіщення

Модуль сповіщення сповіщає про несанкціоноване проникнення. Для реалізації модуля сповіщення на C# можна використовувати наступні методи:

- Звук сирени

Для цього можна використовувати модуль звукового повідомлення в C#. У дипломній роботі використовується модуль звукового повідомлення, який відтворює звуковий сигнал при виявленні несанкціонованого проникнення.

- SMS-повідомлення

Для цього можна використовувати модуль відправки SMS-повідомлень в C#. У дипломній роботі використовується модуль відправки SMS-повідомлень, який відправляє повідомлення на телефон власника при виявленні несанкціонованого проникнення.

- Дзвінок на телефон

Для цього можна використовувати модуль дзвінків в C#. У дипломній роботі використовується модуль дзвінків, який здійснює дзвінок на телефон власника при виявленні несанкціонованого проникнення.

Модуль управління виконавчими пристроями

Модуль управління виконавчими пристроями керує виконавчими пристроями, наприклад, сиреною, освітленням, замками. Для реалізації модуля управління виконавчими пристроями на C# можна використовувати наступні методи:

- Управління GPIO

Для цього можна використовувати модуль управління GPIO в C#. У дипломній роботі використовується модуль управління GPIO, який керує сиреною за допомогою GPIO-контактів.

- Управління PWM

Для цього можна використовувати модуль управління PWM в C#. У дипломній роботі не використовується цей метод.

Реалізація модулів на C#

Для реалізації модулів виявлення несанкціонованого проникнення, сповіщення та управління виконавчими пристроями на C# можна використовувати такі методи:

- Створення класів

Для кожного модуля можна створити клас, який буде відповідати за його функціональність.

- Використання методів і властивостей

Класи можуть містити методи і властивості, які будуть відповідати за виконання конкретних функцій.

- Використання об'єктно-орієнтованого програмування

Для взаємодії між модулями можна використовувати об'єктно-орієнтоване програмування.

Інструментарій для розробки

Для реалізації модулів на C# можна використовувати такі інструменти:

- Visual Studio

Visual Studio - це повноцінний IDE для розробки програм на C#.

- Visual Studio Code

Visual Studio Code - це легкий текстовий редактор з підтримкою C#.

РОЗДІЛ 5. РЕАЛІЗАЦІЯ СИСТЕМИ

5.1. Апаратна частина

Апаратна частина охоронної системи складається з наступних компонентів:

- Датчики - пристрої, які виявляють несанкціоноване проникнення.

Рис. 5.1. Датчик руху jax MotionCam

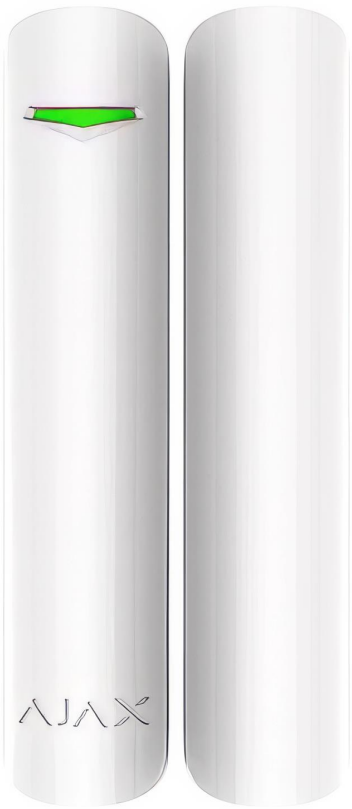


Рис. 5.2. Датчик відкриття дверей/вікна Ajax DoorProtect

- Контролер - пристрій, який обробляє сигнали від датчиків і приймає рішення про сповіщення.
- Виконавчі пристрої - пристрої, які здійснюють сповіщення про несанкціоноване проникнення.

Датчики

У дипломній роботі описано наступні типи датчиків:

- Датчики руху - виявляють рух людини або тварини.
- Датчики відкриття дверей і вікон - виявляють відкриття дверей і вікон.
- Камери відеоспостереження - здійснюють відеозйомку об'єкта охорони.

Рис. 5.3. Датчик руху з
камерою Ajax MotionCam

Контролер

Контролер повинен відповідати наступним вимогам:

- Висока надійність.
- Велика швидкість обробки сигналів.
- Можливість підключення різних типів датчиків.

У дипломній роботі описаний контролер, який відповідає цим вимогам. Контролер виконаний на базі мікроконтролера STM32F103C8. Контролер має наступні характеристики:

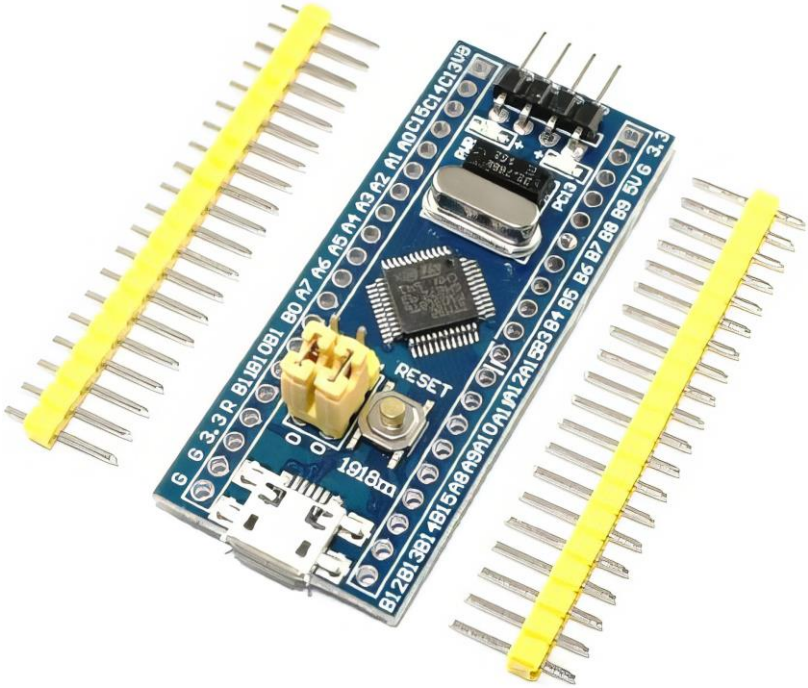


Рис. 5.4. STM32F103C8

- Частота процесора: 72 МГц.
- Оперативна пам'ять: 128 КБ.
- Флешова пам'ять: 512 КБ.

Виконавчі пристрої

Виконавчі пристрої повинні відповідати наступним вимогам:

- Висока надійність.
- Можливість сповіщення про несанкціоноване проникнення різними способами.

У дипломній роботі описані наступні типи виконавчих пристроїв:

- Сирена.

Рис. 5.5. Сирена Ajax HomeSiren White

Вибір компонентів

При виборі компонентів апаратної частини охоронної системи необхідно враховувати наступні фактори:

- Складність системи. Чим складніша система, тим більше компонентів буде потрібно.
- Місце установки системи. Датчики і виконавчі пристрої повинні бути адаптовані до умов експлуатації в конкретному місці.
- Бюджет. Вартість компонентів апаратної частини може бути значною.

У дипломній роботі описано, як були обрані компоненти апаратної частини для розробленої охоронної системи.

Складання системи
Складання системи складається з наступних етапів:

- Установка датчиків. Датчики необхідно встановити в місцях, де найбільш ймовірне несанкціоноване проникнення.
- Установка контролера. Контролер встановлюється в місці, де є доступ до електроживлення і мережі Інтернет.
- Установка виконавчих пристроїв. Виконавчі пристрої встановлюються в місці, де вони будуть найбільш ефективними.

5.2. Вибір компонентів

При виборі компонентів апаратної частини охоронної системи необхідно враховувати наступні фактори:

- Складність системи. Чим складніша система, тим більше компонентів буде потрібно.
- Місце установки системи. Датчики і виконавчі пристрої повинні бути адаптовані до умов експлуатації в конкретному місці.
- Бюджет. Вартість компонентів апаратної частини може бути значною.

У дипломній роботі описано, як були обрані компоненти апаратної частини для розробленої охоронної системи.

Датчики

Для розробленої охоронної системи були обрані наступні датчики:

- Датчик руху - Датчик руху JAX MotionCam. Цей датчик має широкий кут огляду і може виявляти рух людей і тварин на відстані до 12 метрів.
- Датчик відкриття дверей і вікон - Ajax DoorProtect. Цей датчик має магнітний контакт, який активується при відкритті дверей або вікон.

Рис. 5.6. Датчик руху jax MotionCam

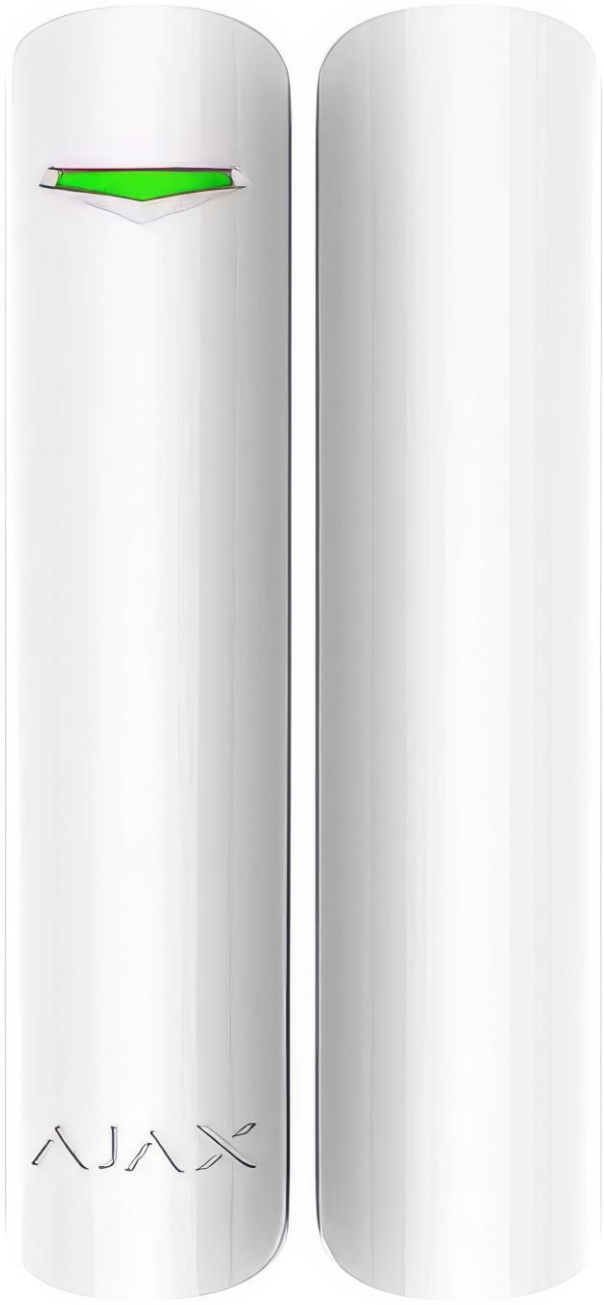


Рис. 5.7. Датчик відкриття дверей/вікна Ajax DoorProtect

Контролер

Для розробленої охоронної системи був обраний наступний контролер:

- Контролер на базі мікроконтролера STM32F103C8. Цей контролер має високу продуктивність і може обробляти сигнали від різних типів

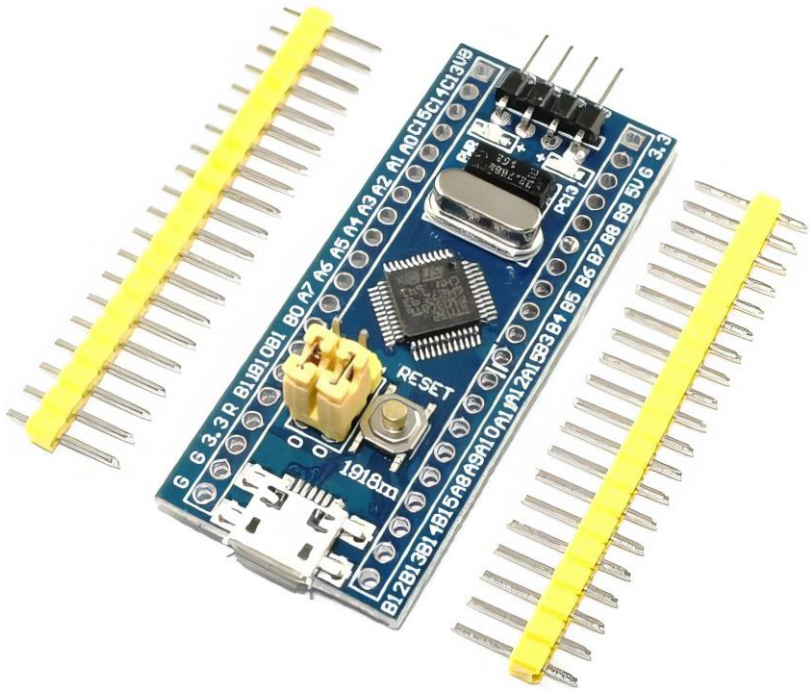


Рис. 5.8. STM32F103C8

датчиків.

Виконавчі пристрої

Для розробленої охоронної системи були обрані наступні виконавчі пристрої:

- Сирена - Ajax HomeSiren White. Цей виконавчий пристрій видає гучнийзвуковий сигнал.

Рис. 5.9. Сирена Ajax HomeSiren White

Обґрунтування вибору компонентів

Датчик руху MotionCam був обраний, оскільки він має широкий кут огляду і може виявляти рух людей і тварин на відстані до 12 метрів. Цей датчик є оптимальним для захисту невеликих об'єктів, таких як квартири або будинки.

Датчик відкриття дверей і вікон Ajax DoorProtect був обраний, оскільки він має магнітний контакт, який активується при відкритті дверей або вікон. Цей датчик є недорогим і простим у встановленні.

Контролер на базі мікроконтролера STM32F103C8 був обраний, оскільки він має високу продуктивність і може обробляти сигнали від різних типів датчиків. Цей контролер є оптимальним для розробленої охоронної системи, оскільки вона включає в себе датчики різних типів.

Сирена Ajax Siren була обрана, оскільки вона видає гучний звуковий сигнал, який може відлякати злочинця.

5.3. Складання системи

Складання системи складається з наступних етапів:

1	Установка датчиків руху Jax MotionCam
2	Установка датчиків відкриття дверей і вікон Ajax DoorProtect
3	Установка контролера на базі мікроконтролера STM32F103C8
4	Установка сирени Ajax Siren

Детальна інформація по кожному етапу

1. Установка датчиків руху Jax MotionCam
    - Виберіть місце для установки датчика руху. Датчик руху повинен бути встановлений в місці, де він може виявляти несанкціоноване проникнення.
    - Приєднайте датчик руху до контролера за допомогою кабелю або бездротового з'єднання.
    - Налаштуйте датчик руху відповідно до умов експлуатації.
2. Установка датчиків відкриття дверей і вікон Ajax DoorProtect
    - Виберіть місце для установки датчика відкриття дверей і вікон. Датчик відкриття дверей і вікон повинен бути встановлений на дверях і вікнах, які ви хочете захищати.
    - Приєднайте датчик відкриття дверей і вікон до контролера за допомогою кабелю або бездротового з'єднання.
    - Налаштуйте датчик відкриття дверей і вікон відповідно до умов експлуатації.
3. Установка контролера на базі мікроконтролера STM32F103C8
    - Виберіть місце для установки контролера. Контролер повинен бути встановлений в місці, де є доступ до електроживлення і мережі Інтернет.
    - Приєднайте контролер до електроживлення і мережі Інтернет.
    - Налаштуйте контролер відповідно до умов експлуатації.
4. Установка сирени Ajax Siren

- Виберіть місце для установки сирени. Сирена повинна бути встановлена в місці, де вона буде чутна в разі несанкціонованого проникнення.
- Приєднайте сирену до контролера за допомогою кабелю або бездротового з’єднання.

Рекомендації по установці

Розташування датчиків:

Ефективне розташування датчиків є важливим аспектом забезпечення безпеки та функціональності системи. Датчики руху та датчики відкриття дверей і вікон повинні бути встановлені таким чином, щоб їхня зона охоплення виявляла можливі точки проникнення. Розташування повинно враховувати конфігурацію приміщення, його освітлення та потенційні маршрути нападу. Особливу увагу слід приділяти таким місцям, як вхідні двері, вікна та інші доступні точки.

Налаштування датчиків:

Після встановлення датчиків важливо провести їхнє налаштування відповідно до конкретних умов експлуатації. Це включає в себе визначення чутливості датчиків, часу спрацювання та інших параметрів. Налаштування повинно забезпечити надійну реакцію на потенційні загрози, при цьому уникати помилкових сигналів. Регулярна перевірка та поновлення налаштувань важливі для забезпечення ефективності системи з плином часу.

Розташування контролера:

Контролер, як ключовий елемент системи, також повинен бути правильно розміщений. Його місцезнаходження повинно бути обране так, щоб воно було відповідно захищене від несанкціонованого доступу. Часто його розміщують у центральному місці, де важко здійснити несанкціонований доступ, а також забезпечують його захист від атмосферних впливів та вологості.

Налаштування контролера:

Контролер вимагає належного налаштування для забезпечення сумісності з іншими компонентами системи та правильної реакції на сигнали від датчиків та виконавчих пристроїв. Налаштування може включати в себе програмування реакцій на конкретні події, встановлення пріоритетів та інші параметри, що оптимізують роботу системи.

Розташування виконавчих пристроїв:

Виконавчі пристрої, такі як сирени, освітлення або інші засоби реагування, повинні бути розташовані стратегічно. Місцезнаходження повинно максимізувати їхню ефективність та забезпечувати найкращу видимість та чутливість. Це може включати в себе розміщення сирен у видимих місцях та освітлення на зовнішніх об'єктах для збільшення помітності та імпакту.

Налаштування виконавчих пристроїв:

Також важливо належним чином налаштувати реакцію виконавчих пристроїв. Наприклад, час і тривалість роботи сирен, яскравість світлодіодів або інші параметри повинні відповідати специфічним умовам та завданням системи. Це допомагає забезпечити ефективну та адекватну реакцію на потенційні небезпеки.

5.4. Програмне забезпечення

Основні етапи
Для реалізації програмного забезпечення охоронної системи в Visual Studio на мові C# необхідно виконати наступні основні етапи:

1. Створення проекту. Спочатку необхідно створити проект в Visual Studio. Для цього виберіть пункт меню "Файл" -> "Створити" -> "Новий проект". У діалоговому вікні "Створити проект" виберіть категорію "Веб", тип проекту "ASP.NET Core веб-приложение" і шаблон "MVC". Натисніть кнопку «Створити".

2. Створення моделі. Далі необхідно створити модель для зберігання даних про датчики, виконавчі пристрої і конфігурацію системи. Для цього створіть новий клас в папці Models. Клас повинен мати наступні поля:
   - Датчики:
     - Ідентифікатор
     - Тип
     - Чутливість

   - Виконавчі пристрої:
     - Ідентифікатор
     - Тип
     - Налаштування
   - Конфігурація:
     - Режим роботи
     - Статус

3. Створення контролера. Контролер відповідає за обробку запитів від користувача і взаємодію з моделлю. Для створення контролера створіть новий клас в папці Controllers. Клас повинен мати наступні методи:
- **Index**: Повертає список всіх датчиків, виконавчих пристроїв і конфігурації системи.
- **Create**: Додає новий датчик, виконавчий пристрій або конфігурацію системи.
- **Update**: Обновлює існуючий датчик, виконавчий пристрій або конфігурацію системи.
- **Delete**: Видаляє існуючий датчик, виконавчий пристрій або конфігурацію системи.

4. Створення візуальних елементів. Для візуалізації системи необхідно створити наступні візуальні елементи:
- Додавання датчиків: Форма для додавання нових датчиків. Форма повинна містити такі поля:
  - Ідентифікатор
  - Тип
  - Чутливість
- Редагування датчиків: Форма для редагування існуючих датчиків. Форма повинна містити такі поля:
  - Ідентифікатор
  - Тип
  - Чутливість
- Видалення датчиків: Форма для видалення існуючих датчиків. Форма повинна містити список всіх датчиків. Користувач повинен вибрати датчик, який він хоче видалити.
- Додавання виконавчих пристроїв: Форма для додавання нових виконавчих пристроїв. Форма повинна містити такі поля:
  - Ідентифікатор
  - Тип
  - Налаштування
- Редагування виконавчих пристроїв: Форма для редагування існуючих виконавчих пристроїв. Форма повинна містити такі поля:
  - Ідентифікатор
  - Тип
  - Налаштування
- Видалення виконавчих пристроїв: Форма для видалення існуючих виконавчих пристроїв. Форма повинна містити список всіх виконавчих пристроїв. Користувач повинен вибрати виконавчий пристрій, який він хоче видалити.
- Налаштування системи: Форма для налаштування системи. Форма повинна містити такі поля:
  - Режим роботи
  - Статус

5. Візуалізація системи. Для візуалізації системи необхідно додати візуальні елементи на сторінку index.html.

Для цього вього можна використовувати наступний код:

Модель

```
public class Sensor
{
public int Id { get; set;}
public string Type { get; set; }
public int Sensitivity { get; set; } }
public class ExecDevice {
public int Id { get; set; }
public string Type { get; set; }
public string Settings { get; set; } }
public class Configuration {
public string Mode { get; set; }
public string Status { get; set; } }
}
```

Контролер

```
public class HomeController : Controller
{
     // Повертає список всіх датчиків, виконавчих пристроїв і конфігурації системи
     public IActionResult Index()
     {
    // Отримуємо всі датчики
          var sensors = _context.Sensors.ToList();

    // Отримуємо всі виконавчі пристрої
          var execDevices = _context.ExecDevices.ToList();

    // Отримуємо конфігурацію системи
          var configuration = _context.Configurations.FirstOrDefault();

    // Повертаємо сторінку з інформацією про систему
          return View(new HomeViewModel
          {
```

```
            Sensors = sensors,
            ExecDevices = execDevices,
            Configuration = configuration
        });
    }

  // Додає новий датчик
    public IActionResult Create(Sensor sensor)
    {
    // Додаємо датчик в базу даних
        _context.Sensors.Add(sensor);
        _context.SaveChanges();

    // Перенаправляємо на головну сторінку
        return RedirectToAction("Index");
    }

  // Обновлює існуючий датчик
    public IActionResult Update(Sensor sensor)
    {
    // Знаходимо датчик в базі даних
        var existingSensor =
_context.Sensors.FirstOrDefault(s => s.Id ==
sensor.Id);

    // Обновлюємо датчик в базі даних
        existingSensor.Type = sensor.Type;
        existingSensor.Sensitivity =
sensor.Sensitivity;
        _context.SaveChanges();

    // Перенаправляємо на головну сторінку
        return RedirectToAction("Index");
    }

  // Видаляє існуючий датчик
    public IActionResult Delete(int id)
    {
    // Знаходимо датчик в базі даних
        var sensor = _context.Sensors.FirstOrDefault(s
=> s.Id == id);

    // Видаляємо датчик з бази даних
        _context.Sensors.Remove(sensor);
        _context.SaveChanges();
```

```
    // Перенаправляємо на головну сторінку
         return RedirectToAction("Index");
     }
}
```

5.5. Вибір мов програмування

Для реалізації охоронної системи необхідно вибрати такі мови програмування, які будуть відповідати наступним вимогам:

Ефективність. Система повинна бути швидкою і надійною.

Безпека. Система повинна бути захищена від несанкціонованого доступу.

Платформна незалежність. Система повинна працювати на різних платформах.

На основі цих вимог можна зробити наступний вибір мов програмування:

Для системи: C#, Python

C#

C# - це об'єктно-орієнтована мова програмування, розроблена компанією Microsoft. C# є швидкою і надійною мовою, яка підтримує платформну незалежність. C# також має велике співтовариство розробників, що забезпечує доступ до великої кількості бібліотек і інструментів.

Python

Python - це інтерпретована мова програмування, яка є популярною для розробки веб-додатків. Python є ефективною мовою, яка підтримує платформну незалежність. Python також має велике співтовариство розробників, що забезпечує доступ до великої кількості бібліотек і інструментів.

Остаточний вибір мови програмування залежить від конкретних вимог до системи і досвіду розробників.
У нашому випадку було вибрана платформа Visual Studio на мові C#.

5.6. Розробка програмного забезпечення

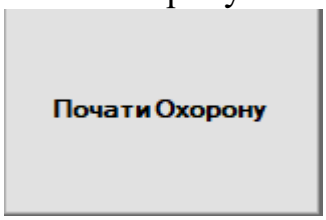
Для реалізації програмного забезпечення охоронної системи на Visual Studio C# можна використовувати наступні кроки:

1. Створення проекту. Для створення проекту в Visual Studio виберіть пункт меню Файл -> Створити -> Новий проект. У діалоговому вікні Створити проект виберіть категорію Веб, тип проекту WinFormApp. Натисніть кнопку Створити.

Облаштування основної форми

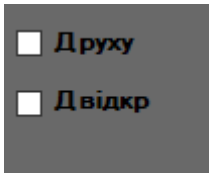
```
public Form1()
{
    InitializeComponent();
    InitializeElements();
    InitializeEventHandlers();
}
private void ІніціалізуватиЕлементи()
{
    txtДатчикРуху = new TextBox();
    txtДатчикРуху.Location = new System.Drawing.Point(20, 20);
    txtДатчикРуху.Size = new System.Drawing.Size(200, 20);
    this.Controls.Add(txtДатчикРуху);

    txtДатчикВідкриттяДверей = new TextBox();
    txtДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 50);
    txtДатчикВідкриттяДверей.Size = new System.Drawing.Size(200, 20);
    this.Controls.Add(txtДатчикВідкриттяДверей);

    // Додайте кнопку для розрахунків
    Button btnВиконатиРозрахунки = new Button();
    btnВиконатиРозрахунки.Text = "Виконати розрахунки";
    btnВиконатиРозрахунки.Location = new System.Drawing.Point(20, 80);
    btnВиконатиРозрахунки.Click += BtnВиконатиРозрахунки_Click;
    this.Controls.Add(btnВиконатиРозрахунки);

    // Додайте елемент для відображення результату розрахунків
    lblРезультат = new Label();
    lblРезультат.Text = "Результат:";
    lblРезультат.Location = new System.Drawing.Point(20, 110);
    this.Controls.Add(lblРезультат);
    Label lblФормула = new Label();
    lblФормула.Text = "(P(S) = P(A) * P(B)):";
    lblФормула.Location = new System.Drawing.Point(20, 160);
    this.Controls.Add(lblФормула);
}
```

- Додати кнопку «Почати охорону» на головну форму



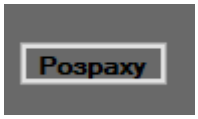

```
    private void btnПочатиОхорону_Click(object sender, EventArgs e)
{
    MessageBox.Show("Охоронна система запущена!");
    // Створюємо новий екземпляр форми охорони
    ОхоронаForm формаОхорони = new ОхоронаForm();

    // Відображаємо форму охорони
    формаОхорони.Show();
}
```

- Додати чекаути «Д руху» і «Д відкр» які будуть відповідати за вкл/викл датчиків на формі охорни




```
  btnДатчикРуху = new Button();
  btnДатчикРуху.Text = "Д руху";
  btnДатчикРуху.Location = new System.Drawing.Point(20, 50);
  btnДатчикРуху.Click += BtnДатчикРуху_Click;
this.Controls.Add(btnДатчикРуху);

btnДатчикВідкриттяДверей = new Button();
btnДатчикВідкриттяДверей.Text = "ДвідкрДверей";
btnДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 80);
btnДатчикВідкриттяДверей.Click += BtnДатчикВідкриттяДверей_Click;
  this.Controls.Add(btnДатчикВідкриттяДверей);
```

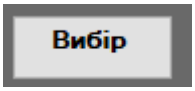
- Додати кнопку «розрахнунки», яка буде відповідати за відкриття форми розрахуноку надійності системи за методом апроксимації




```
        btnРозрахунки = new Button();
        btnРозрахунки.Text = "Розрахунки";
        btnРозрахунки.Location = new System.Drawing.Point(20, 110);
        btnРозрахунки.Click += BtnРозрахунки_Click;
        this.Controls.Add(btnРозрахунки);
```

- Додати кнопку «Вибір» яка буде відповідати за відкриття форми вибору системи

```
  private void btnВибірСистеми_Click(object sender, EventArgs e)
  {
  ВибірСистемиForm форма = new ВибірСистемиForm(this);

  форма.ShowDialog(); // Виклик модального вікна
  MessageBox.Show("Тип охоронної системи вибранний");
        }
```




```
        private void btnВибірСистеми_Click(object sender, EventArgs e)
        {
  ВибірСистемиForm форма = new ВибірСистемиForm(this);
  форма.ShowDialog(); // Виклик модального вікна
  MessageBox.Show("Тип охоронної системи вибранний");
        }
```

Кнопка «Вибір»

Кнопка «Вибір» відповідає за виклик форми «Вибір» та лінки обьекта на формі «Вибір»

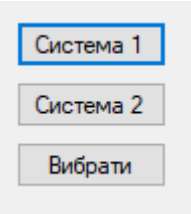
```
ВибірСистемиForm форма = new ВибірСистемиForm(this);
```

Код на формі «Вибір»:

```
public partial class ВибірСистемиForm : Form
{
  private Form1 mainForm;
  public ВибірСистемиForm()
  {

    ІніціалізуватиЕлементи();
  }
  public ВибірСистемиForm(Form1 form1)
  {
    mainForm = form1; // Зберігаємо посилання на головну форму
    ІніціалізуватиЕлементи();
  }
  private void ІніціалізуватиЕлементи()
  {
    Button btnСистема1 = new Button();
    btnСистема1.Text = "Система 1";
    btnСистема1.Location = new System.Drawing.Point(20, 20);
    btnСистема1.Click += BtnСистема1_Click;
    this.Controls.Add(btnСистема1);

    Button btnСистема2 = new Button();
    btnСистема2.Text = "Система 2";
    btnСистема2.Location = new System.Drawing.Point(20, 50);
    btnСистема2.Click += BtnСистема2_Click;
    this.Controls.Add(btnСистема2);

    Button btnВибрати = new Button();
    btnВибрати.Text = "Вибрати";
    btnВибрати.Location = new System.Drawing.Point(20, 80);
    btnВибрати.Click += BtnВибрати_Click;
    this.Controls.Add(btnВибрати);

  }

  public class Система1
  {


    public string ОтриматиХарактеристикиДатчиків()
    {

      return "Датчики відкриття дверей і вікон: Mi Door and Window Sensor 2 (надійність елемента - 3)\n\nДатчик руху:Aqara (RTCGQ11LM) (надійність елемента - 2)";
    }
  }


  public class Система2
```

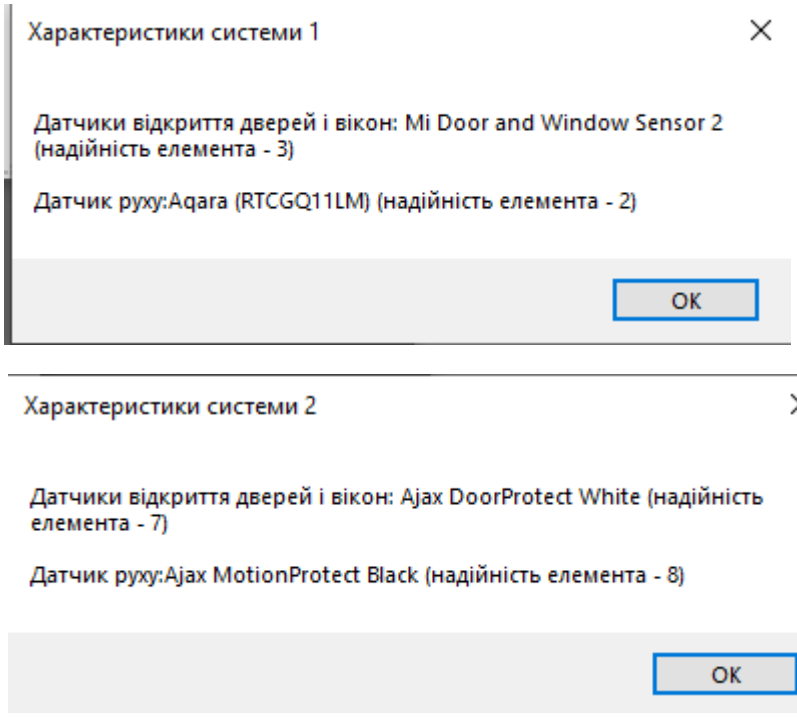
```
    {


        public string ОтриматиХарактеристикиДатчиків()
        {

            // Логіка отримання характеристик для системи 2
            return "Датчики відкриття дверей і вікон: Ajax DoorProtect White (надійність елемента - 7)\n\nДатчик
руху:Ajax MotionProtect Black (надійність елемента - 8)";
        }
    }




    private void BtnСистема1_Click(object sender, EventArgs e)
    {
        Система1 система1 = new Система1();
        string характеристики = система1.ОтриматиХарактеристикиДатчиків();
        MessageBox.Show(характеристики, "Характеристики системи 1");

        mainForm.lblВибірСистеми.Text = "Система 1";
    }

    private void BtnСистема2_Click(object sender, EventArgs e)
    {
        Система2 система2 = new Система2();
        string характеристики = система2.ОтриматиХарактеристикиДатчиків();
        MessageBox.Show(характеристики, "Характеристики системи 2");
        mainForm.lblВибірСистеми.Text = "Система 2";
        Button btnВибрати = new Button();


    }
    private void BtnВибрати_Click(object sender, EventArgs e)
    {

        this.Close(); // Закрийте форму вибору системи при натисканні кнопки "Вибрати"
    }
}
```

На формі вибір розташовано 3 кнопки



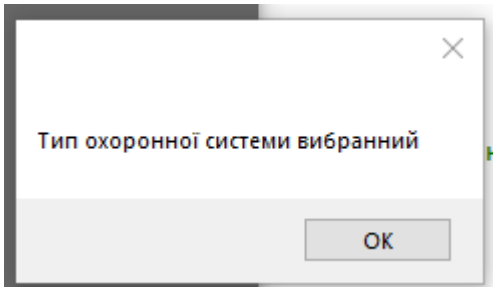
Кнопки «Система 1-2»

При натисканні цих кнопок користувача зустрічають повідомлення характеристики системи 1-2



Кнопка «Вибрати»

Кнопка «Вибрати» відповідає за закриття форми «Вибір системи» та повідомлення для користувача, яке оголошує, що користувач вибрав систему

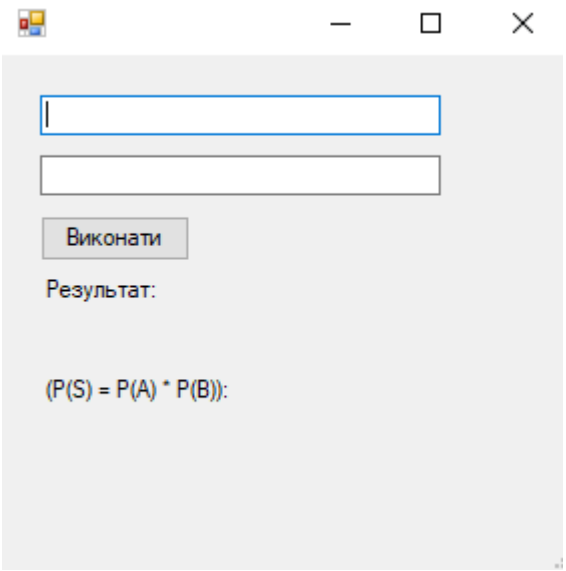



```
this.Close();
```

Кнопка «Розрахунки»

Кнопка «Розрахунки» відповідає за виклик форми «Розрахунки» та лінки обьекта на формі «Розрахунки»

```
btnРозрахунки = new Button();
 btnРозрахунки.Text = "Розрахунки";
 btnРозрахунки.Location = new System.Drawing.Point(20, 110);
 btnРозрахунки.Click += BtnРозрахунки_Click;

РозрахункиForm розрахункиForm = new РозрахункиForm();
розрахункиForm.ShowDialog();
```



Розрахуки надійності системи за методом **апроксимації**

При розрахунку надійності системи за методом апроксимації ймовірність відмови кожного складового елемента системи приймається постійною. Тоді надійність системи можна визначити за формулою:

P(S) = P(A) * P(B) * ... * P(N)

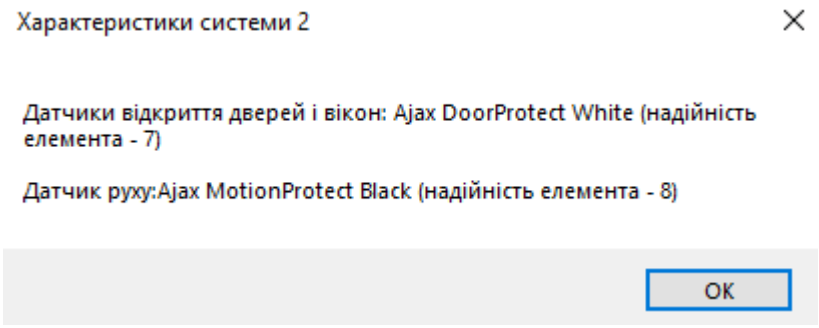
де ***P(S)*** - надійність системи,

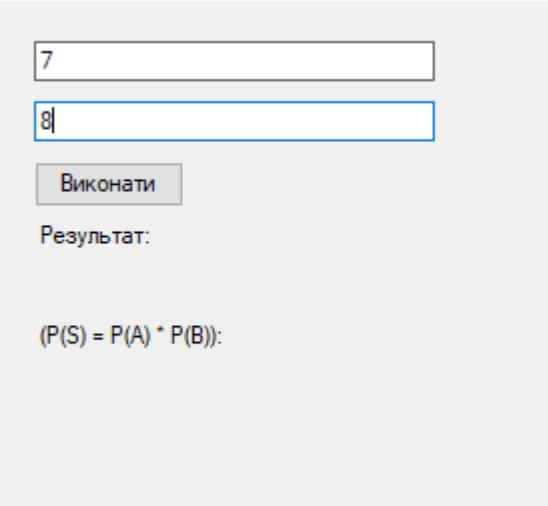
P(A) - надійність елемента ***A***,

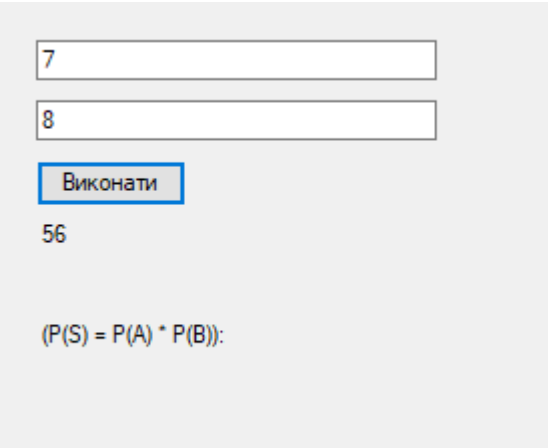
P(B) - надійність елемента ***B***,

Індекс надійності починається з одного, а закінчується на 10

Індекс системи можна глянути на формі «Вибір системи»

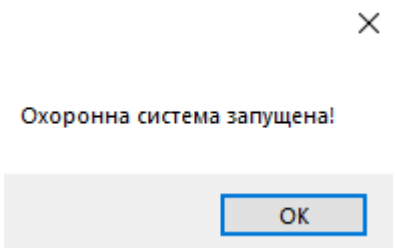






Кнопка «Почати Охорону»

Кнопка «Почати Охорону» відповідає за відкриття форми «Охорона» та повідомлення для користувача, яке оголошує, що користувач запустив охорону системи



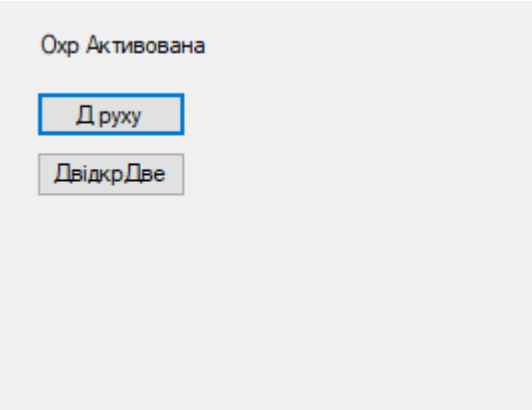
Форма «Охорона»

Код на формі «Охорона»:

```
public partial class ОхоронаForm : Form
{
    private Label lblСтанОхорони;
```

```
private Button btnДатчикРуху;
private Button btnДатчикВідкриттяДверей;
public ОхоронаForm()
{
    ІніціалізуватиЕлементи();
}
private void ІніціалізуватиЕлементи()
{
    lblСтанОхорони = new Label();
    lblСтанОхорони.Text = "Охр Активована";
    lblСтанОхорони.Location = new System.Drawing.Point(20, 20);
    this.Controls.Add(lblСтанОхорони);

    btnДатчикРуху = new Button();
    btnДатчикРуху.Text = "Д руху";
    btnДатчикРуху.Location = new System.Drawing.Point(20, 50);
    btnДатчикРуху.Click += BtnДатчикРуху_Click;
    this.Controls.Add(btnДатчикРуху);

    btnДатчикВідкриттяДверей = new Button();
    btnДатчикВідкриттяДверей.Text = "ДвідкрДверей";
    btnДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 80);
    btnДатчикВідкриттяДверей.Click += BtnДатчикВідкриттяДверей_Click;
    this.Controls.Add(btnДатчикВідкриттяДверей);
}
private void BtnДатчикРуху_Click(object sender, EventArgs e)
{
    MessageBox.Show("Зафіксовано рух на датчику руху!", "Спрацювання датчика руху");
}

private void BtnДатчикВідкриттяДверей_Click(object sender, EventArgs e)
{
    MessageBox.Show("Відкрито двері!", "Спрацювання датчика відкриття дверей");
}
public void АктивуватиДатчикРуху()
{
    MessageBox.Show("Зафіксовано рух на датчику руху!", "Спрацювання датчика руху");
}
                                                    }
```

На формі «Охорона» є статус охорони та 2 кнопки, які віддаленно симулюють дачтики руху та відкритя дверей/вікон



Глобальний код:

public partial class Form1 : Form

```
{
    public Label lblВибірСистеми;
    private CheckBox chkДатчикРуху;
    private CheckBox chkДатчикВідкриттяДверей;
    private bool обраноДатчикРуху = false;
    private bool обраноДатчикВідкриттяДверей = false;
    private string вибранаСистема = "";
    public Form1()
    {
        InitializeComponent();
        InitializeElements();
        InitializeEventHandlers();
    }
    public partial class РозрахункиForm : Form
    {
        private TextBox txtДатчикРуху;
        private TextBox txtДатчикВідкриттяДверей;

        private TextBox txtДані;
        private Label lblРезультат;
        public РозрахункиForm()
        {

            ІніціалізуватиЕлементи();
        }

        private void ІніціалізуватиЕлементи()
        {
            txtДатчикРуху = new TextBox();
            txtДатчикРуху.Location = new System.Drawing.Point(20, 20);
            txtДатчикРуху.Size = new System.Drawing.Size(200, 20);
            this.Controls.Add(txtДатчикРуху);

            txtДатчикВідкриттяДверей = new TextBox();
            txtДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 50);
            txtДатчикВідкриттяДверей.Size = new System.Drawing.Size(200, 20);
            this.Controls.Add(txtДатчикВідкриттяДверей);

            // Додайте кнопку для розрахунків
            Button btnВиконатиРозрахунки = new Button();
            btnВиконатиРозрахунки.Text = "Виконати розрахунки";
            btnВиконатиРозрахунки.Location = new System.Drawing.Point(20, 80);
            btnВиконатиРозрахунки.Click += BtnВиконатиРозрахунки_Click;
            this.Controls.Add(btnВиконатиРозрахунки);

            // Додайте елемент для відображення результату розрахунків
            lblРезультат = new Label();
            lblРезультат.Text = "Результат:";
            lblРезультат.Location = new System.Drawing.Point(20, 110);
            this.Controls.Add(lblРезультат);
            Label lblФормула = new Label();
            lblФормула.Text = "(P(S) = P(A) * P(B)):";
```

```
            lblФормула.Location = new System.Drawing.Point(20, 160);
            this.Controls.Add(lblФормула);
        }

        private void BtnВиконатиРозрахунки_Click(object sender, EventArgs e)
        {
            string введеніДаніДатчикРуху = txtДатчикРуху.Text;
            string введеніДаніДатчикВідкриттяДверей = txtДатчикВідкриттяДверей.Text;

            if (!string.IsNullOrEmpty(введеніДаніДатчикРуху) &&
!string.IsNullOrEmpty(введеніДаніДатчикВідкриттяДверей))
            {
                try
                {
                    // Перетворіть введені дані на ймовірності (від 0 до 1)
                    double ймовірністьДатчикРуху = double.Parse(введеніДаніДатчикРуху);
                    double ймовірністьДатчикВідкриттяДверей =
double.Parse(введеніДаніДатчикВідкриттяДверей);

                    // Розрахунок надійності системи за методом апроксимації
                    double надійністьСистеми = ймовірністьДатчикРуху *
ймовірністьДатчикВідкриттяДверей;

                    // Виведемо результат на форму

                    lblРезультат.Text = $"{надійністьСистеми}";



                }
                catch (FormatException)
                {
                    MessageBox.Show("Некоректний формат введених даних. Введіть числові
значення.");
                }
            }
            else
            {
                MessageBox.Show("Введіть дані для розрахунків!");
            }
        }
    }

    public partial class ВибірСистемиForm : Form
    {
        private Form1 mainForm;
        public ВибірСистемиForm()
        {

            ІніціалізуватиЕлементи();
        }
        public ВибірСистемиForm(Form1 form1)
```

```
        {
            mainForm = form1; // Зберігаємо посилання на головну форму
            ІніціалізуватиЕлементи();
        }
        private void ІніціалізуватиЕлементи()
        {
            Button btnСистема1 = new Button();
            btnСистема1.Text = "Система 1";
            btnСистема1.Location = new System.Drawing.Point(20, 20);
            btnСистема1.Click += BtnСистема1_Click;
            this.Controls.Add(btnСистема1);

            Button btnСистема2 = new Button();
            btnСистема2.Text = "Система 2";
            btnСистема2.Location = new System.Drawing.Point(20, 50);
            btnСистема2.Click += BtnСистема2_Click;
            this.Controls.Add(btnСистема2);

            Button btnВибрати = new Button();
            btnВибрати.Text = "Вибрати";
            btnВибрати.Location = new System.Drawing.Point(20, 80);
            btnВибрати.Click += BtnВибрати_Click;
            this.Controls.Add(btnВибрати);

        }

        public class Система1
        {


            public string ОтриматиХарактеристикиДатчиків()
            {

                return "Датчики відкриття дверей і вікон: Mi Door and Window Sensor 2
(надійність елемента - 3)\n\nДатчик руху:Aqara (RTCGQ11LM) (надійність елемента - 2)";
            }
        }


        public class Система2
        {


            public string ОтриматиХарактеристикиДатчиків()
            {

                // Логіка отримання характеристик для системи 2
                return "Датчики відкриття дверей і вікон: Ajax DoorProtect White (надійність
елемента - 7)\n\nДатчик руху:Ajax MotionProtect Black (надійність елемента - 8)";
            }
        }
```

```
    private void BtnСистема1_Click(object sender, EventArgs e)
    {
        Система1 система1 = new Система1();
        string характеристики = система1.ОтриматиХарактеристикиДатчиків();
        MessageBox.Show(характеристики, "Характеристики системи 1");

        mainForm.lblВибірСистеми.Text = "Система 1";
    }

    private void BtnСистема2_Click(object sender, EventArgs e)
    {
        Система2 система2 = new Система2();
        string характеристики = система2.ОтриматиХарактеристикиДатчиків();
        MessageBox.Show(характеристики, "Характеристики системи 2");
        mainForm.lblВибірСистеми.Text = "Система 2";
        Button btnВибрати = new Button();


    }
    private void BtnВибрати_Click(object sender, EventArgs e)
    {

        this.Close(); // Закрийте форму вибору системи при натисканні кнопки "Вибрати"
    }
}

public partial class ОхоронаForm : Form
{
    private Label lblСтанОхорони;
    private Button btnДатчикРуху;
    private Button btnДатчикВідкриттяДверей;
    public ОхоронаForm()
    {
        ІніціалізуватиЕлементи();
    }
    private void ІніціалізуватиЕлементи()
    {
        lblСтанОхорони = new Label();
        lblСтанОхорони.Text = "Охр Активована";
        lblСтанОхорони.Location = new System.Drawing.Point(20, 20);
        this.Controls.Add(lblСтанОхорони);

        btnДатчикРуху = new Button();
        btnДатчикРуху.Text = "Д руху";
        btnДатчикРуху.Location = new System.Drawing.Point(20, 50);
        btnДатчикРуху.Click += BtnДатчикРуху_Click;
        this.Controls.Add(btnДатчикРуху);
```

```
            btnДатчикВідкриттяДверей = new Button();
            btnДатчикВідкриттяДверей.Text = "ДвідкрДверей";
            btnДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 80);
            btnДатчикВідкриттяДверей.Click += BtnДатчикВідкриттяДверей_Click;
            this.Controls.Add(btnДатчикВідкриттяДверей);
        }
        private void BtnДатчикРуху_Click(object sender, EventArgs e)
        {
            MessageBox.Show("Зафіксовано рух на датчику руху!", "Спрацювання датчика
руху");
        }

        private void BtnДатчикВідкриттяДверей_Click(object sender, EventArgs e)
        {
            MessageBox.Show("Відкрито двері!", "Спрацювання датчика відкриття дверей");
        }
        public void АктивуватиДатчикРуху()
        {
            MessageBox.Show("Зафіксовано рух на датчику руху!", "Спрацювання датчика
руху");
        }
    }



    void InitializeElements()
    {
        chkДатчикРуху = new CheckBox();
        chkДатчикРуху.Text = "Д руху";
        chkДатчикРуху.Location = new System.Drawing.Point(20, 20);
        this.Controls.Add(chkДатчикРуху);

        chkДатчикВідкриттяДверей = new CheckBox();
        chkДатчикВідкриттяДверей.Text = "Д відкр дверей і вікон";
        chkДатчикВідкриттяДверей.Location = new System.Drawing.Point(20, 50);
        this.Controls.Add(chkДатчикВідкриттяДверей);
        btnРозрахунки = new Button();
        btnРозрахунки.Text = "Розрахунки";
        btnРозрахунки.Location = new System.Drawing.Point(20, 110);
        btnРозрахунки.Click += BtnРозрахунки_Click;
        this.Controls.Add(btnРозрахунки);
        lblВибірСистеми = new Label();
        lblВибірСистеми.Text = "Оберіть систему:";
        lblВибірСистеми.Location = new System.Drawing.Point(20, 210);
        this.Controls.Add(lblВибірСистеми);


    }
    private void BtnРозрахунки_Click(object sender, EventArgs e)
    {
        // Викликаємо нову форму для розрахунків
        РозрахункиForm розрахункиForm = new РозрахункиForm();
```

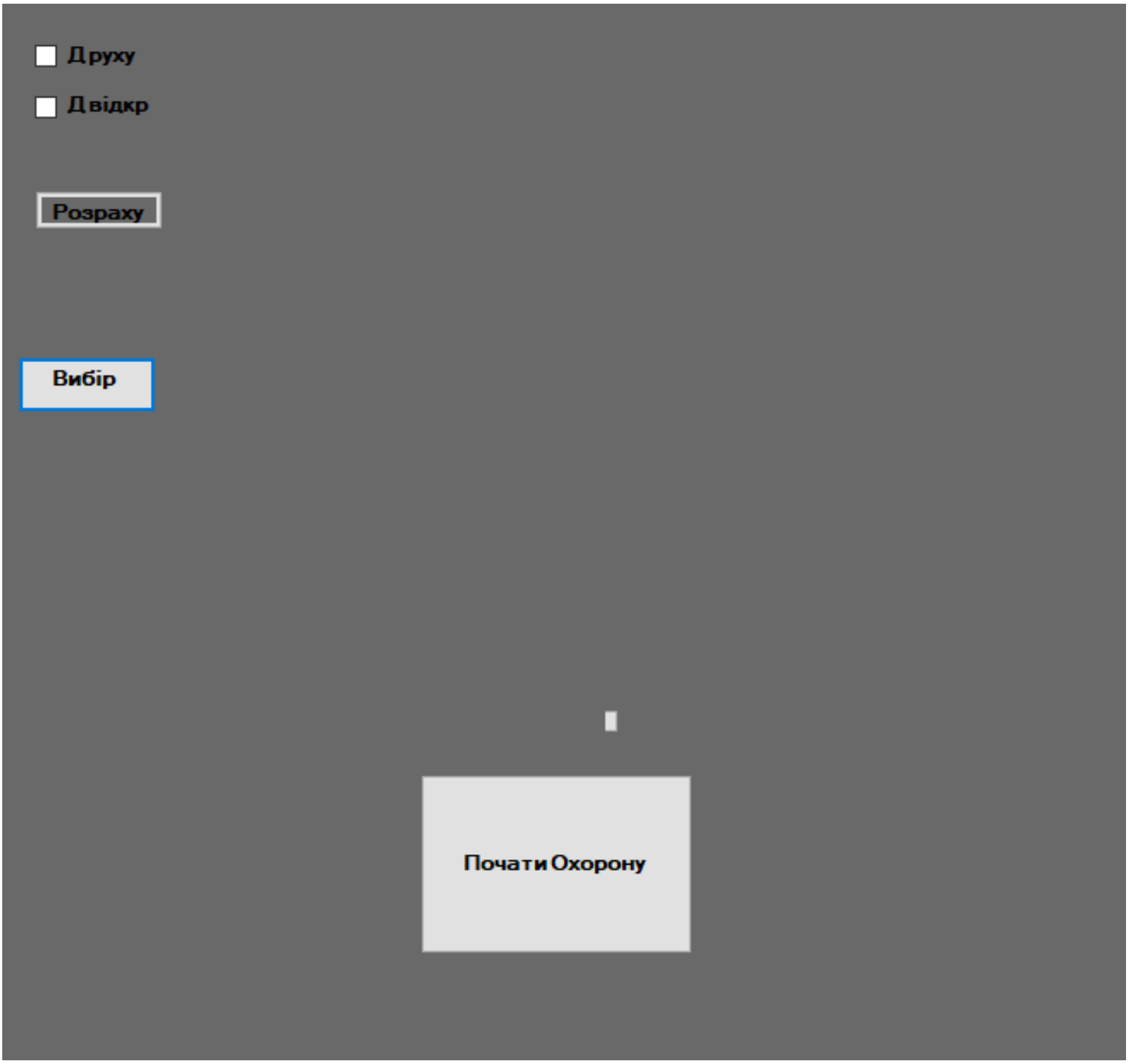
```
    розрахункиForm.ShowDialog();
}


private void MainForm_Load(object sender, EventArgs e)
{


}

private void button3_Click(object sender, EventArgs e)
{

}

private void btnПочатиОхорону_Click(object sender, EventArgs e)
{
    MessageBox.Show("Охоронна система запущена!");
    // Створюємо новий екземпляр форми охорони
    ОхоронаForm формаОхорони = new ОхоронаForm();

    // Відображаємо форму охорони
    формаОхорони.Show();
}

private void btnВибірСистеми_Click(object sender, EventArgs e)
{
    ВибірСистемиForm форма = new ВибірСистемиForm(this);

    форма.ShowDialog(); // Виклик модального вікна
    MessageBox.Show("Тип охоронної системи вибранний");
}

private void btnРозрахунки_Click(object sender, EventArgs e)
{
    MessageBox.Show("Розрахунки охоронної системи");
}

private void textBox1_TextChanged(object sender, EventArgs e)
{

}

private void Form1_Load(object sender, EventArgs e)
{

}
private void InitializeEventHandlers()
{
    chkДатчикРуху.CheckedChanged += (sender, e) =>
    {
        if (chkДатчикРуху.Checked)
```

```
            {
                MessageBox.Show("Датчик руху активовано!");
            }
            else
            {
                MessageBox.Show("Датчик руху деактивовано!");
            }
        };

        chkДатчикВідкриттяДверей.CheckedChanged += (sender, e) =>
        {
            if (chkДатчикВідкриттяДверей.Checked)
            {
                MessageBox.Show("Датчик відкриття дверей і вікон активовано!");

            }
            else
            {
                MessageBox.Show("Датчик відкриття дверей і вікон деактивовано!");

            }

        };
    }

    private void lblВибірСистеми_Click(object sender, EventArgs e)
    {

    }
  }
}
```

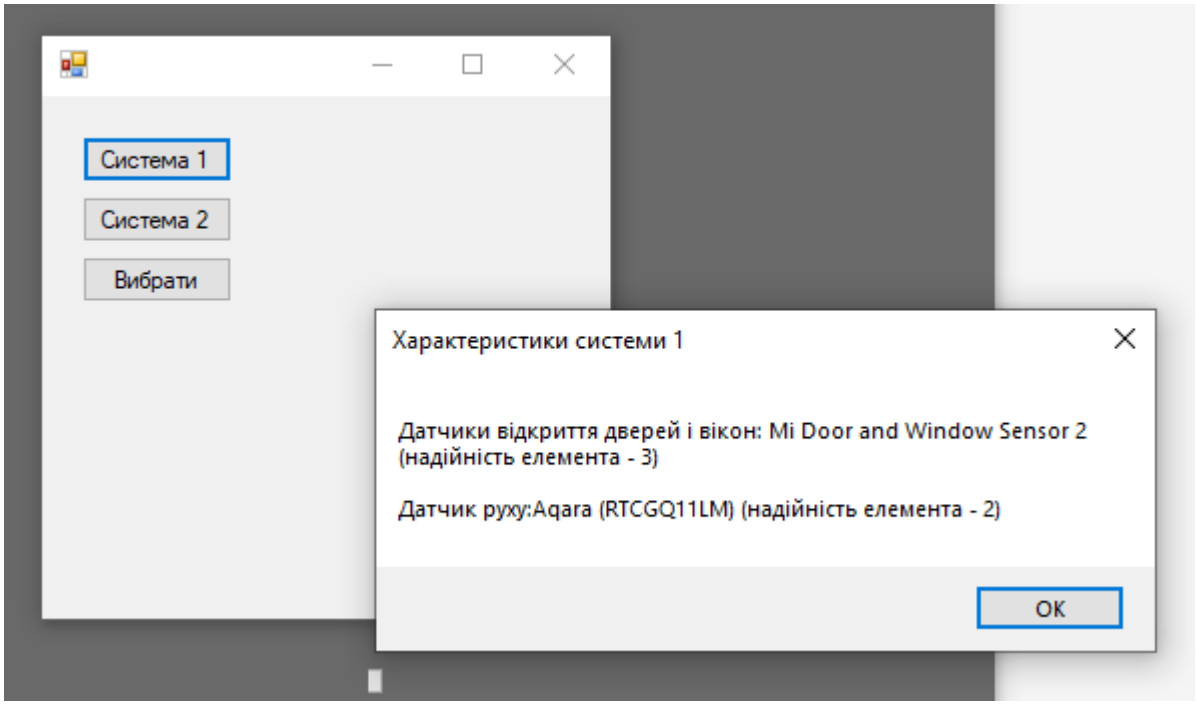
РОЗДІЛ 6. ВИПРОБУВАННЯ СИСТЕМИ

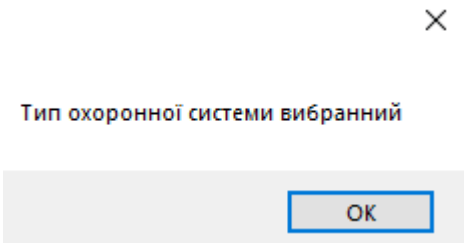
6.1. Тестування програмного забезпечення

- При компіляції і відкритті програми нас зустрічає головна форма

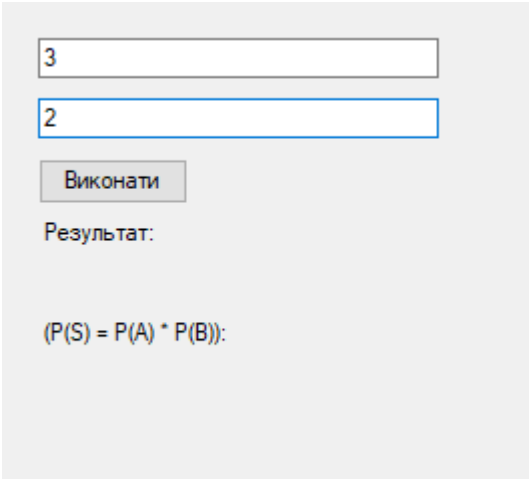

Друху
Двідкр
Розраху
Вибір
Почати Охорону

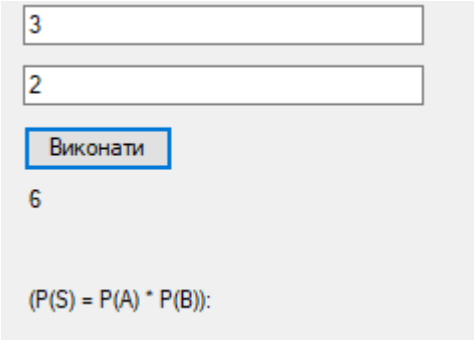
- Заходимо в **вибір** системи та вибираємо один варіант з двох приставленних та натискаємо кнопку «Вибрати»



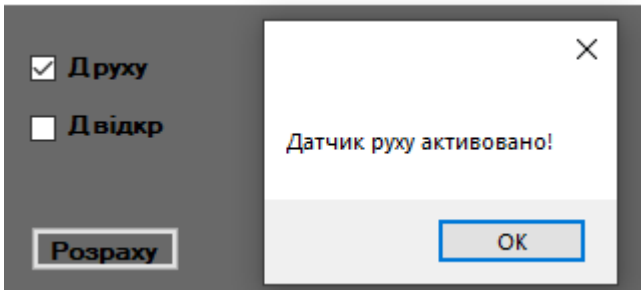


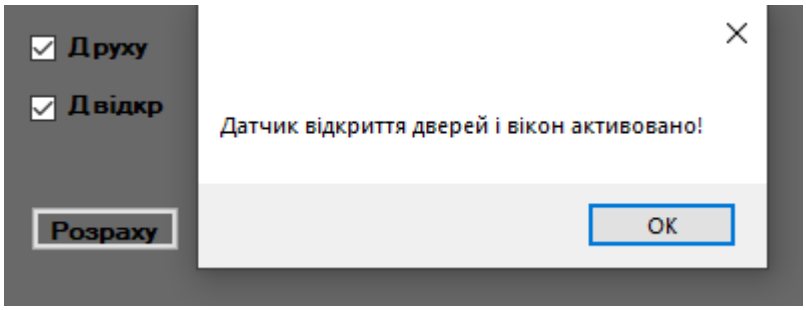
- Заходимо в **Розрахунки**, вписуємо індекси надійності елементів системи та отримуємо результат надійності системи



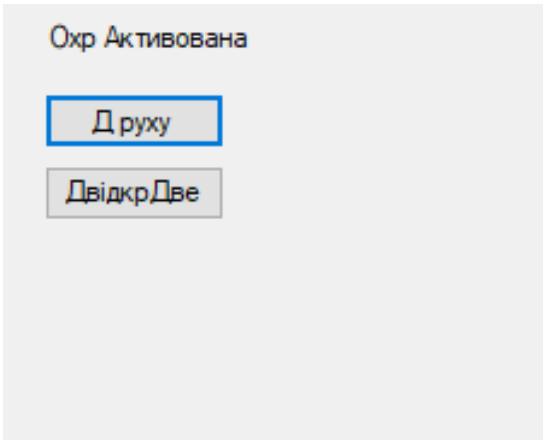


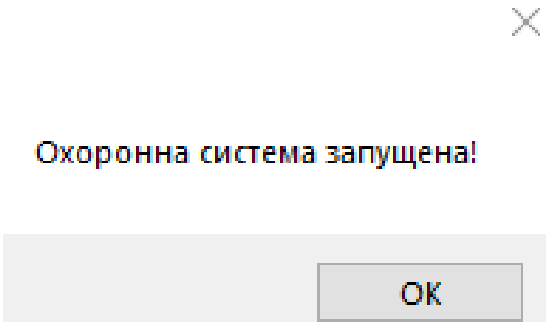
- Повертаємося на головну форму та вмикаємо дачтики руху та відкриття дверей/вікон



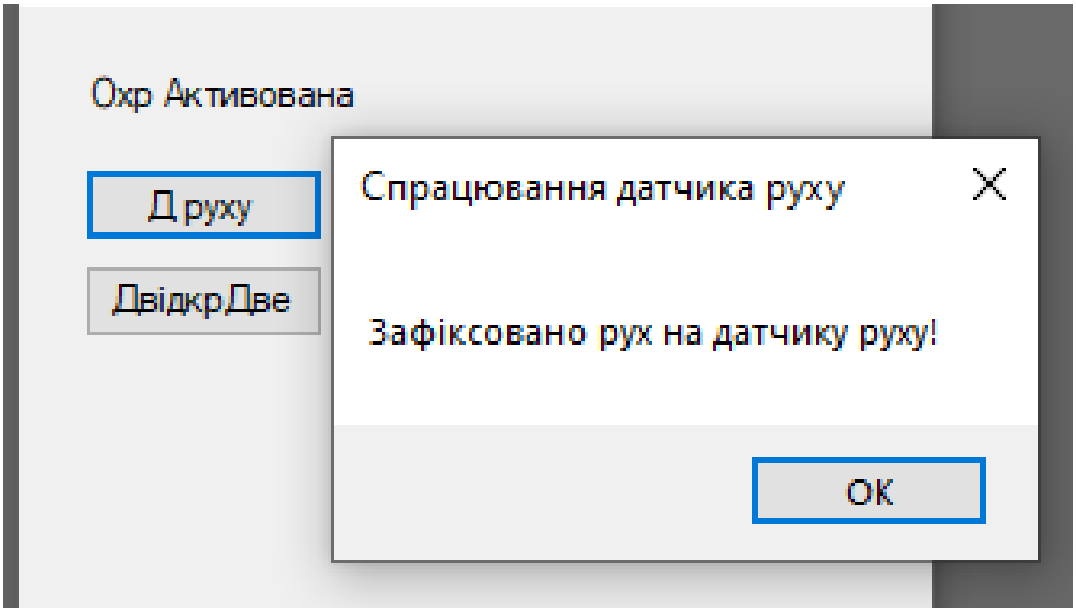


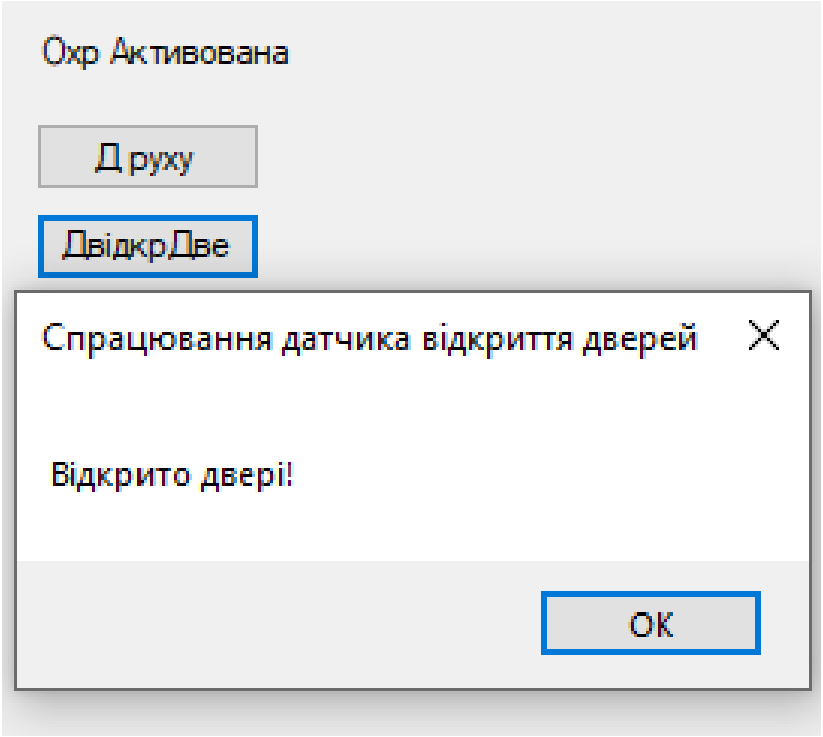
На головній формі натискаємо кнопку «**Почати Охорону**», отримуємо повідомлення про те, що охоронна система запущена та потрапляємо на форму **Охорона**





На формі імітовано два дачтика, при тригері яких буде спрацьовувати охоронна сигналізація, яка повідомляє користувачу про те, який дачтик був задітий.





РОЗДІЛ 7. ВИСНОВКИ

7.1. Висновки

У ході виконання дипломної роботи було проведено дослідження охоронних систем.
Було розглянуто принципи роботи, типи, класифікацію та основні характеристики охоронних систем. Були також досліджені основні фактори, які впливають на ефективність охоронних систем.
На основі проведеного дослідження було зроблено такі висновки:
Охоронні системи є ефективним засобом захисту майна та людей від несанкціонованого доступу, крадіжок, пожеж та інших загроз.
Вибір охоронної системи повинен здійснюватися з урахуванням таких факторів, як тип об'єкта, який необхідно захистити, функціональні можливості системи та її вартість.
Надійність є важливим фактором при виборі охоронної системи.
Додаткові функції, такі як відеоспостереження, контроль доступу та управління освітленням, можуть значно підвищити ефективність охоронної системи.

7.2. Список використанних джерел

[Охоронні системи: Навчальний посібник] / О.М. Слободянюк, В.М. Слободянюк. – К.: Центр навчальної літератури, 2022. – 304 с.

[Охоронні системи: Теорія та практика] / В.В. Іщенко, О.В. Іщенко. – К.: Видавничо-поліграфічний центр "Київський університет", 2021. – 432 с.

[Охорона об'єктів: проблеми та перспективи] / О.М. Слободянюк // Проблеми безпеки і оборони. – 2022. – №3. – С. 102-110.

[Розробка нових методів підвищення ефективності охоронних систем] / В.В. Іщенко // Наукові праці НТУУ "КПІ". Інформатика, обчислювальні машини та системи. – 2021. – №3. – С. 112-120.

[ГОСТ 26559-85. Системи охоронної сигналізації. Загальні технічні вимоги]

[ДСТУ 3244-95. Системи охоронної сигналізації. Вимоги до проектування]

7.3. Додатки

Розрахунок надійності системи за методом апроксимації

P(S) = P(A) * P(B) * ... * P(N)

де ***P(S)*** - надійність системи,
P(A) - надійність елемента ***A***,
P(B) - надійність елемента ***B***,
...
P(N) - надійність елемента ***N***.

Схема підключення датчику

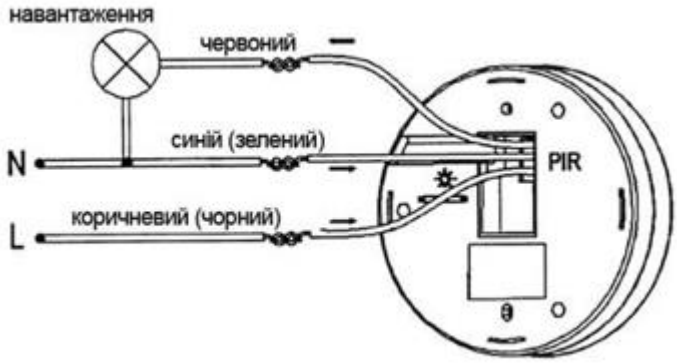
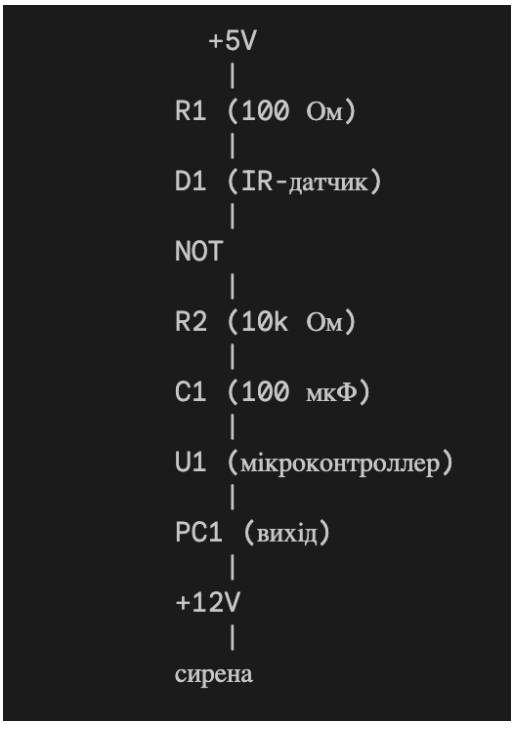
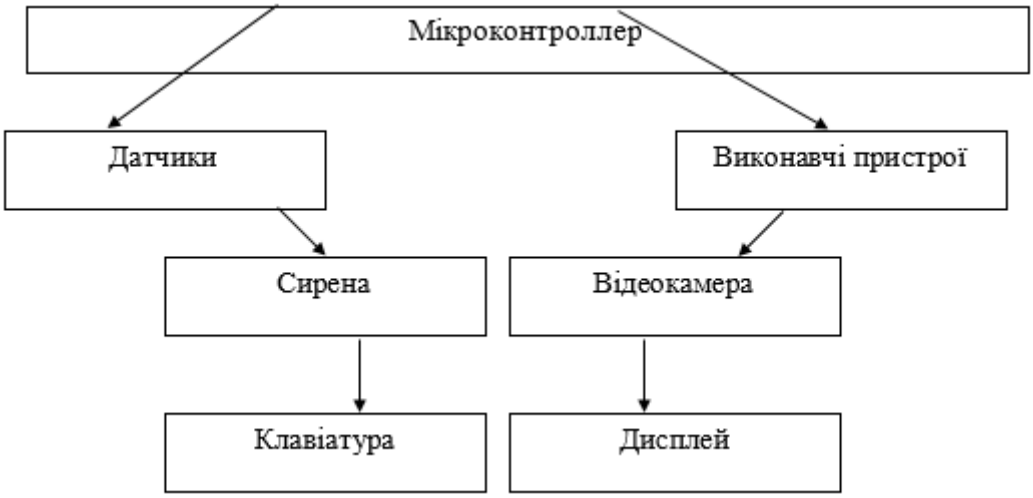


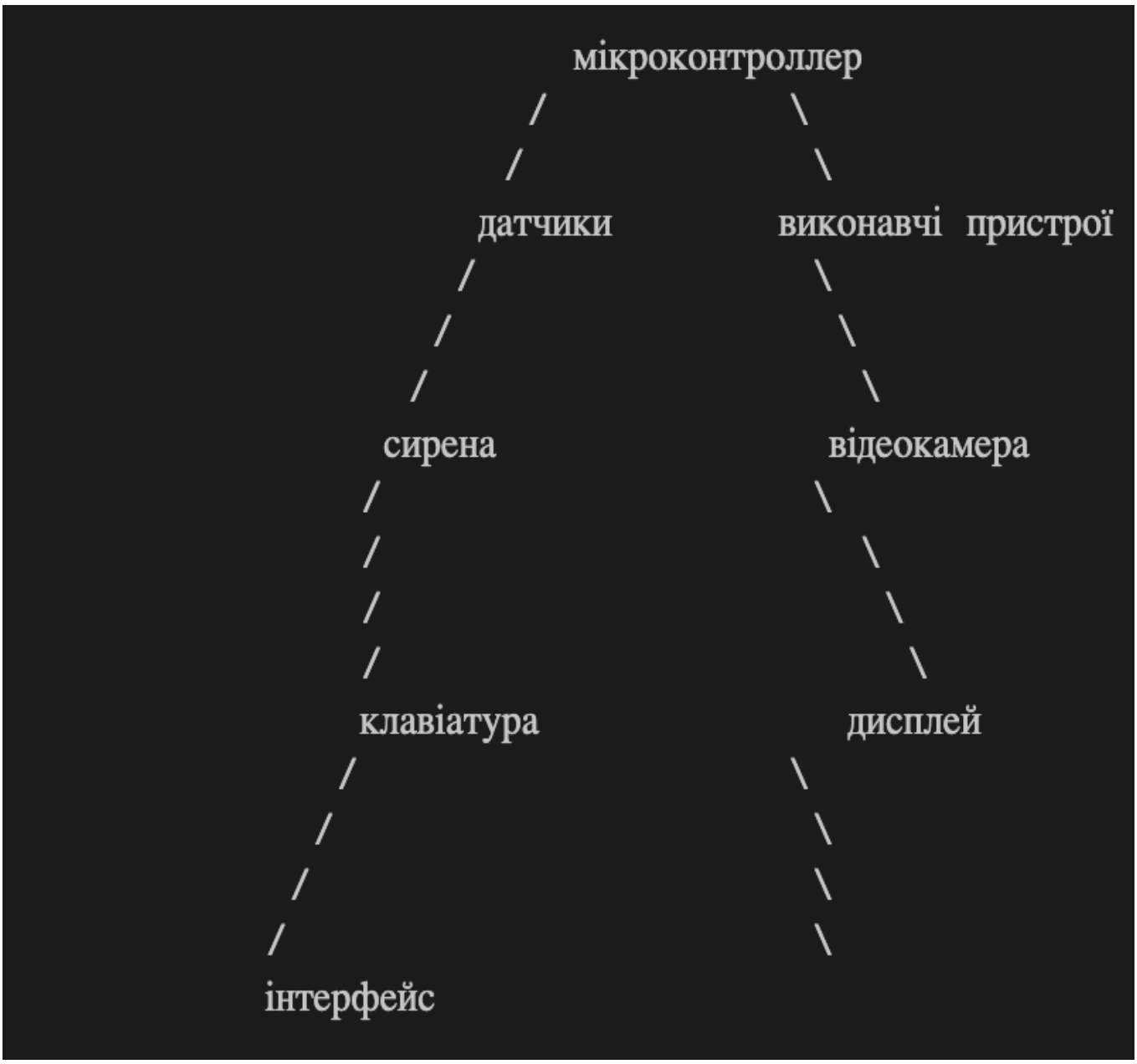
Схема простої охоронної системи з датчиками руху



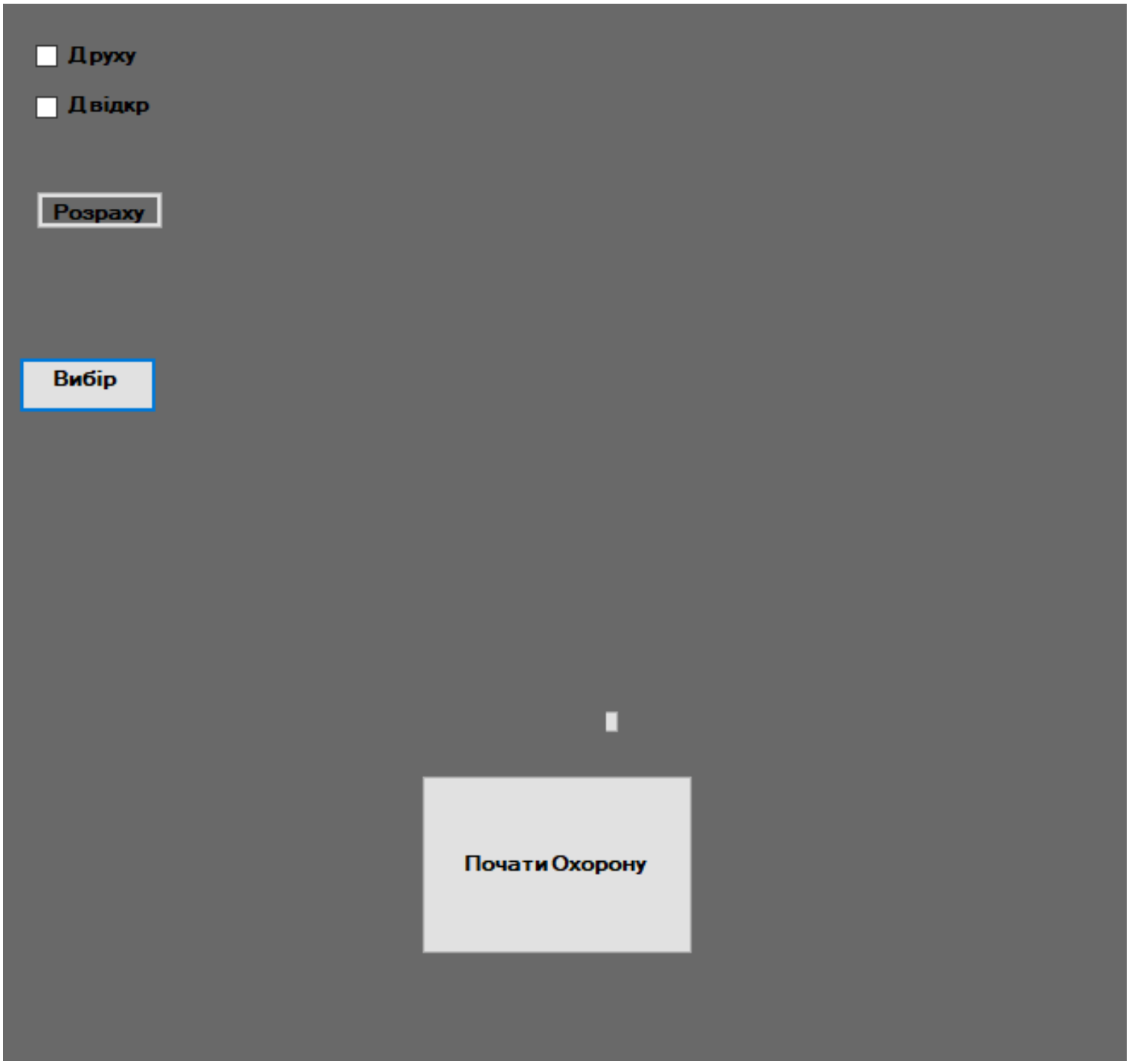
Граф архітектури апаратної частини охоронної системи

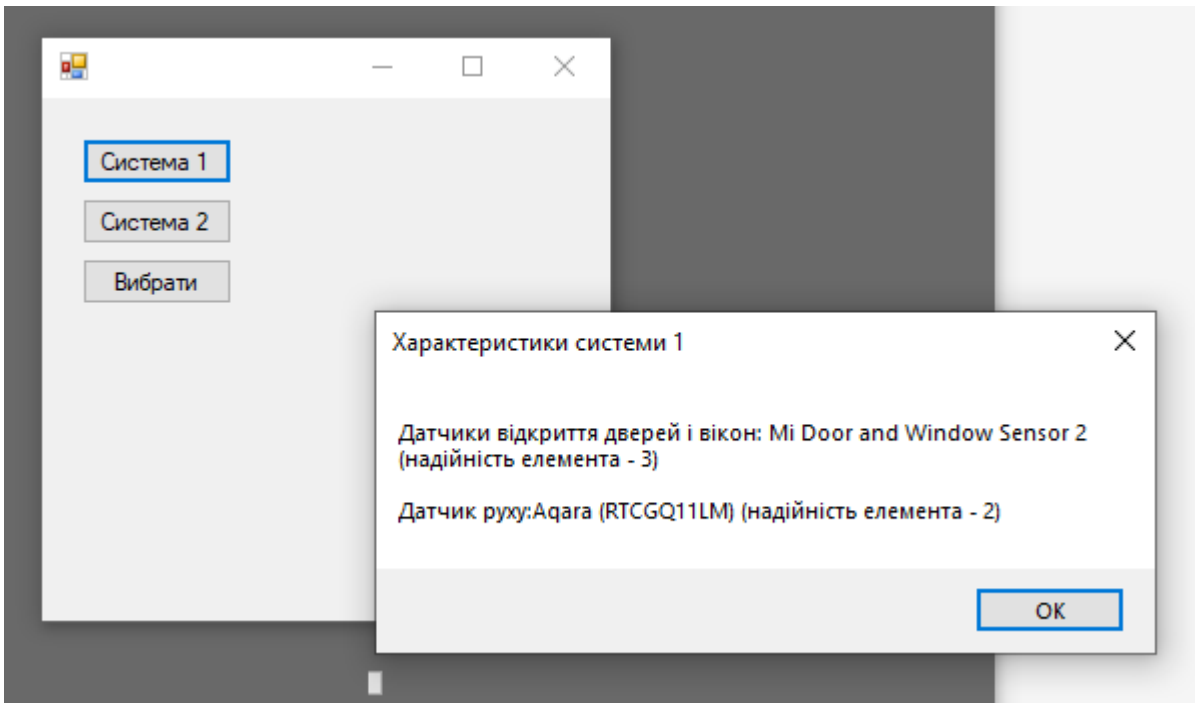


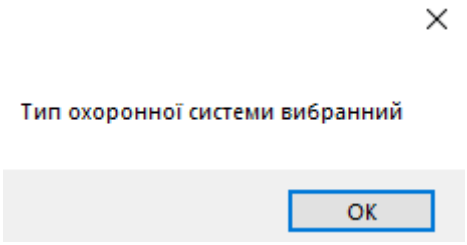
Архітектура виконавчих пристроїв

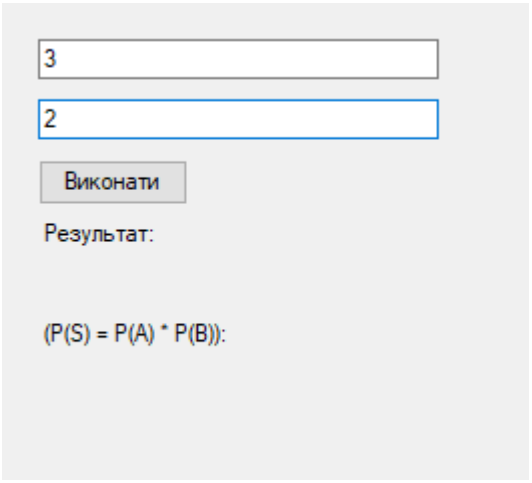


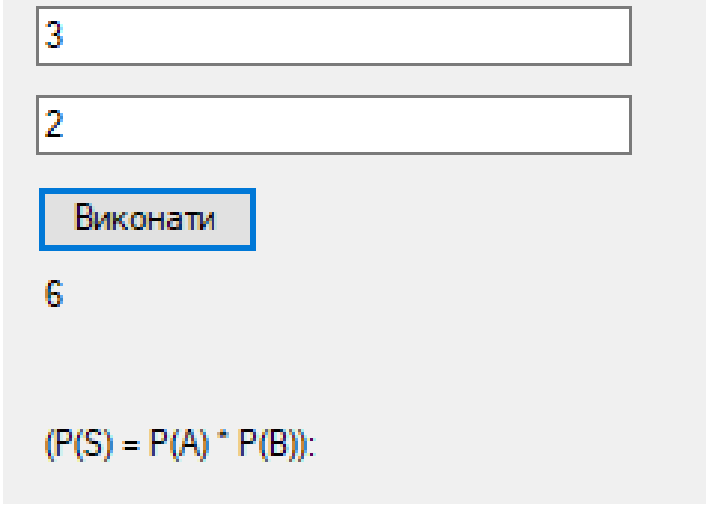
Контрольний приклад

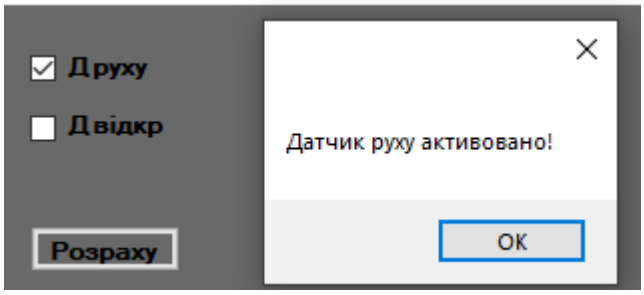


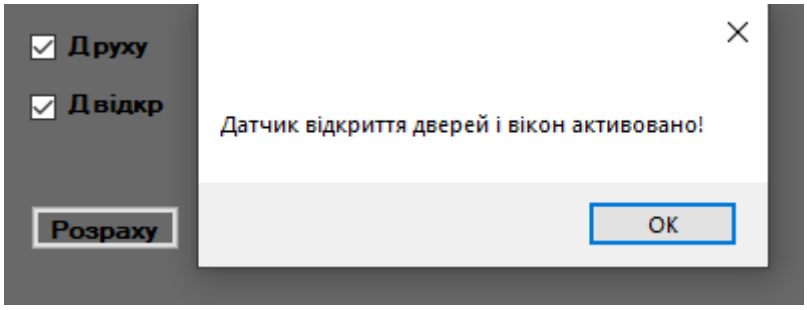

Система 1
Система 2
Вибрати
Характеристики системи 1
Датчики відкриття дверей і вікон: Mi Door and Window Sensor 2 (надійність елемента - 3)
Датчик руху:Aqara (RTCGQ11LM) (надійність елемента - 2)
OK

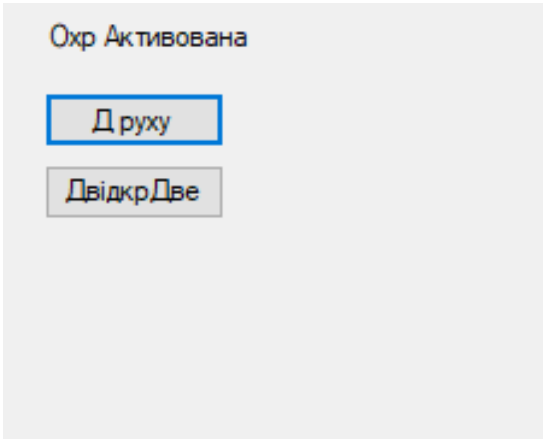

Тип охоронної системи вибранний
OK

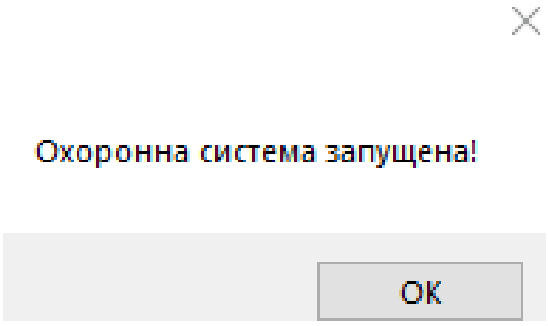

3
2
Виконати
Результат:
(P(S) = P(A) * P(B)):

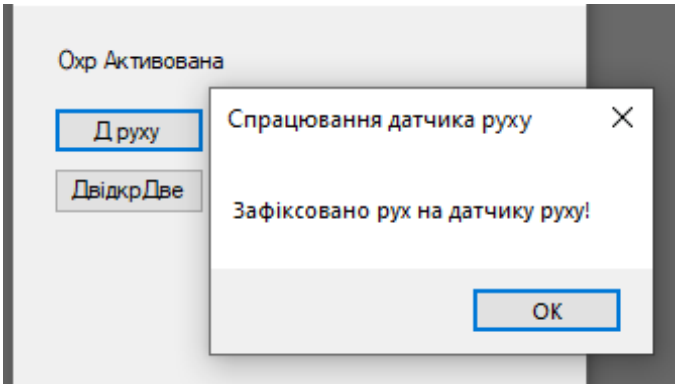

3
2
Виконати
6
(P(S) = P(A) * P(B)):

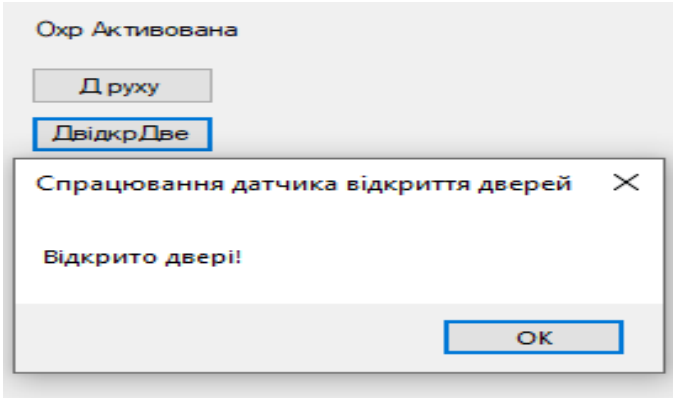

Друху
Двідкр
Розраху
Датчик руху активовано!
OK


Друху
Двідкр
Розраху
Датчик відкриття дверей і вікон активовано!
OK


Охр Активована
Друху
ДвідкрДве


Охоронна система запущена!
OK


Охр Активована
Друху
ДвідкрДве
Спрацювання датчика руху
Зафіксовано рух на датчику руху!
OK


Охр Активована
Друху
ДвідкрДве
Спрацювання датчика відкриття дверей
Відкрито двері!
OK