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

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-01

Дипломний проект

здобувача освіти денної форми навчання
КБ.01.01.000.ДП

АРШЕР
МИКОЛА ВІКТОРОВИЧ

м. Одеса
2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-01**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка системи охоронної сигналізації підприємства на основі технології Arduino

Проектний матеріал складається з пояснювальної записки на 80 сторінках та графічного (презентаційного) матеріалу на 14 аркушах (слайдах).

Дипломник _____ (Аршер М.В.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічного розділу _____ (Іванченков В.С.)

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «17» 06 2024 р. Протокол ДКК № 1

Оцінка ЕК 4 (добре) 77 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"16" 09 2024 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти Аршер Миколі Вікторовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Розробка системи охоронної сигналізації підприємства на основі технології Arduino

затверджена наказом по коледжу від "02" листопада 2023 р. № 224

2. Термін здачі закінченого проекту (роботи)

3. Вихідні данні до проекту (роботи):

Об'єкт аналізу – система охоронної сигналізації як елемент ТЗО

Основні датчики – магнітні, руху, диму, вуглекислого газу, протікання води

Технологія розробки – Arduino UNO

Кількість складових в напрямку масштабованості систем сигналізації - 9

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Розглянути проблеми створення системи охоронної сигналізації для підприємства. Навести вимоги до технічних засобів охорони. Розглянути складові технічних засобів охорони. Провести аналіз принципів роботи датчиків охоронної сигналізації, розглянути їх типи та класи Розробити систему ОС на основі Arduino UNO. Навести економічну частине та охорону праці.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Актуальність теми; Ефективність технічних засобів охорони об'єктів; Компоненти системи охоронної сигналізації підприємства; Різновиди охоронних датчиків; Зовнішній вигляд датчиків руху; Розміщення датчиків та обладнання охоронної сигналізації в приміщеннях підприємства; Макет електричної схеми системи охоронної сигналізації підприємства; Алгоритм дій при роботі з Arduino IDE; Плати мікроконтролера ArduinoUNO; Перевірка роботи програмного забезпечення та електричної схеми. Tinkercad; Висновки

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

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

7. Дата видачі завдання 15 січня 2024 р.

Керівник *Стайкуца С.В.* (підпис)

Завдання прийняв до виконання *Аршер М.В.* (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	*Вступ. Постановка задачі проектування*	*29.04.24-2.05.24*	Виконав
2.	*Аналіз технічного завдання та пошук літератури*	*2.05.24-4.05.24*	Виконав
3.	*Дослідження вимог до технічних засобів охорони*	*4.05.24-10.05.24*	Виконав
4.	*Аналіз складових ТЗО;*	*10.05.24-15.05.24*	Виконав
5.	*Дослідження типів датчиків в системах сигналізації;*	*15.05.24-19.05.24*	Виконав
6.	*Складання технічного завдання на розробку*	*19.05.24-23.05.24*	Виконав
7.	*Обґрунтування вибору платформи Arduino для розробки системи охоронної сигналізації підприємства*	*19.05.22-25.05.24*	Виконав
8.	*Розробка системи схеми охоронної системи сигналізації*		Виконав
9.	*ПЗ для завантаження мікроконтролера Arduino UNO*	*25.05.24-29.05.24*	Виконав
10.	*Виконання економічних розрахунків*	*29.05.24-2.06.24*	Виконав
11.	*Розробка питань з охорони праці та техніки безпеки*	*2.06.24-6.06.24*	Виконав
12.	*Підготовка мультимедійної презентації проекту*	*06.06.24-09.06.24*	Виконав

Дипломник (підпис)

Керівник (підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 01. 01 000. 00 ДП	Дипломний проект		
А4			КБ 01. 01 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 01. 01 000. 00 ДП		
Розробив		Аршер М.В.			Розробка системи охоронної сигналізації підприємства на основі технології Arduino	Літ.	Аркуш 4 / Аркушів 80
Перевірив		Стайкуца С.В.				НДП	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.4КБ-01	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

У сучасному світі, що швидко розвивається, питання безпеки мають першорядне значення як для окремих осіб, так і для компаній. Потреба в надійних заходах безпеки, починаючи від захисту будинків і закінчуючи охороною комерційних установ, ніколи не була такою критичною. Серед різноманітних доступних рішень безпеки охоронна сигналізація виділяється як один із найефективніших засобів запобігання несанкціонованому доступу та стримування потенційних зловмисників.

Охоронна сигналізація, також відома як охоронна сигналізація або охоронна сигналізація, - це електронні пристрої, призначені для виявлення несанкціонованого проникнення в приміщення або зону обмеженого доступу. Ці сигналізації працюють, виявляючи рух, відкривання дверей чи вікон, розбиття скла чи інші ознаки вторгнення, ініціюючи тривогу для сповіщення мешканців або персоналу служби безпеки. Основне завдання сигналізації про вторгнення – діяти як стримуючий фактор для потенційних зловмисників і сповіщати органи влади у разі порушення.

Сигналізація відіграє вирішальну роль у захисті будинків, малих підприємств та інших цінних активів від несанкціонованого доступу та вторгнень. Завдяки широкому спектру датчиків, передовій технології та можливостям інтеграції сучасні системи охоронної сигналізації пропонують комплексні рішення безпеки, адаптовані до унікальних потреб кожного об’єкта. Інвестуючи в систему охоронної сигналізації та залишаючись в курсі останніх досягнень у технологіях безпеки, окремі особи та компанії можуть покращити свою безпеку та насолоджуватися більшим душевним спокоєм у світі, що стає все більш невизначеним. При цьому розробка власних рішень на базі відкритих протоколів та технологій, наприклад, Arduino, сьогодні є досить актуальним питанням.

1 ОСНОВНА ЧАСТИНА

1.1 Огляд проблеми створення системи охоронної сигналізації для підприємства

1.1.1 Вимоги до технічних засобів охорони

Вимоги до технічних засобів охорони визначаються враховуючи різноманітні аспекти інформаційної безпеки, включаючи конфіденційність, цілісність, доступність та відповідність до вимог законодавства та стандартів. Ось деякі загальні вимоги: надійність; безпека; сумісність; ефективність; масштабованість; простота управління; шифрування даних; захист від витоку інформації; резервне копіювання і відновлення; автоматизація; спроможність до аналізу та аудиту; відповідність до вимог законодавства та стандартів.

Запобіжні заходи та вимоги до технічних засобів охорони повинні бути розроблені з урахуванням конкретних потреб інформаційної безпеки кожної організації або системи.

Технічні засоби повинні бути надійними і функціонувати без збоїв у важливі моменти. Це є одним з найважливіших аспектів в інформаційній безпеці. Це особливо важливо в критичних ситуаціях, коли недоступність або несправність систем може призвести до серйозних проблем. Ось деякі важливі аспекти надійності технічних засобів:

1) стійкість до витоку даних: технічні засоби повинні бути захищені від витоку конфіденційної інформації через вразливості програмного забезпечення, атаки ззовні або недбале оброблення даних;

2) стійкість до внутрішніх помилок: системи повинні мати вбудовані механізми виявлення помилок і відновлення роботи в разі виявлення неполадок;

3) резервне копіювання та відновлення: засоби повинні мати механізми для створення резервних копій даних та відновлення роботи систем в разі втрати даних або несправності обладнання;

4) моніторинг та попередження: системи повинні вести постійний моніторинг стану засобів та вчасно сповіщати про можливі проблеми або вразливості;

5) резервування та дублювання: використання дублювання обладнання, мереж та інших критичних систем для забезпечення безперервності роботи в разі відмови одного з елементів;

6) автоматизація відновлення роботи систем після виявлення відмови або витоку даних;

7) стійкість до кібератак: засоби повинні мати вбудовані механізми захисту від різних типів кібератак та здатність протистояти їм без збоїв;

8) тестування та аудит: регулярне тестування, аудит та аналіз безпеки для виявлення потенційних проблем та вдосконалення систем безпеки.

Надійність технічних засобів охорони є основою для забезпечення безперебійної та безпечної роботи інформаційних систем. Вона дозволяє підприємствам та організаціям ефективно захищати свою інформацію від загроз та непередбачених ситуацій.

Засоби повинні забезпечувати високий рівень захисту від різноманітних загроз, включаючи кібератаки, витік інформації, внутрішні та зовнішні загрози тощо. Безпека технічних засобів охорони є одним з найважливіших аспектів в інформаційній безпеці. Засоби повинні забезпечувати високий рівень захисту від різноманітних загроз, які можуть ставити під загрозу конфіденційність, цілісність та доступність інформації та ресурсів.

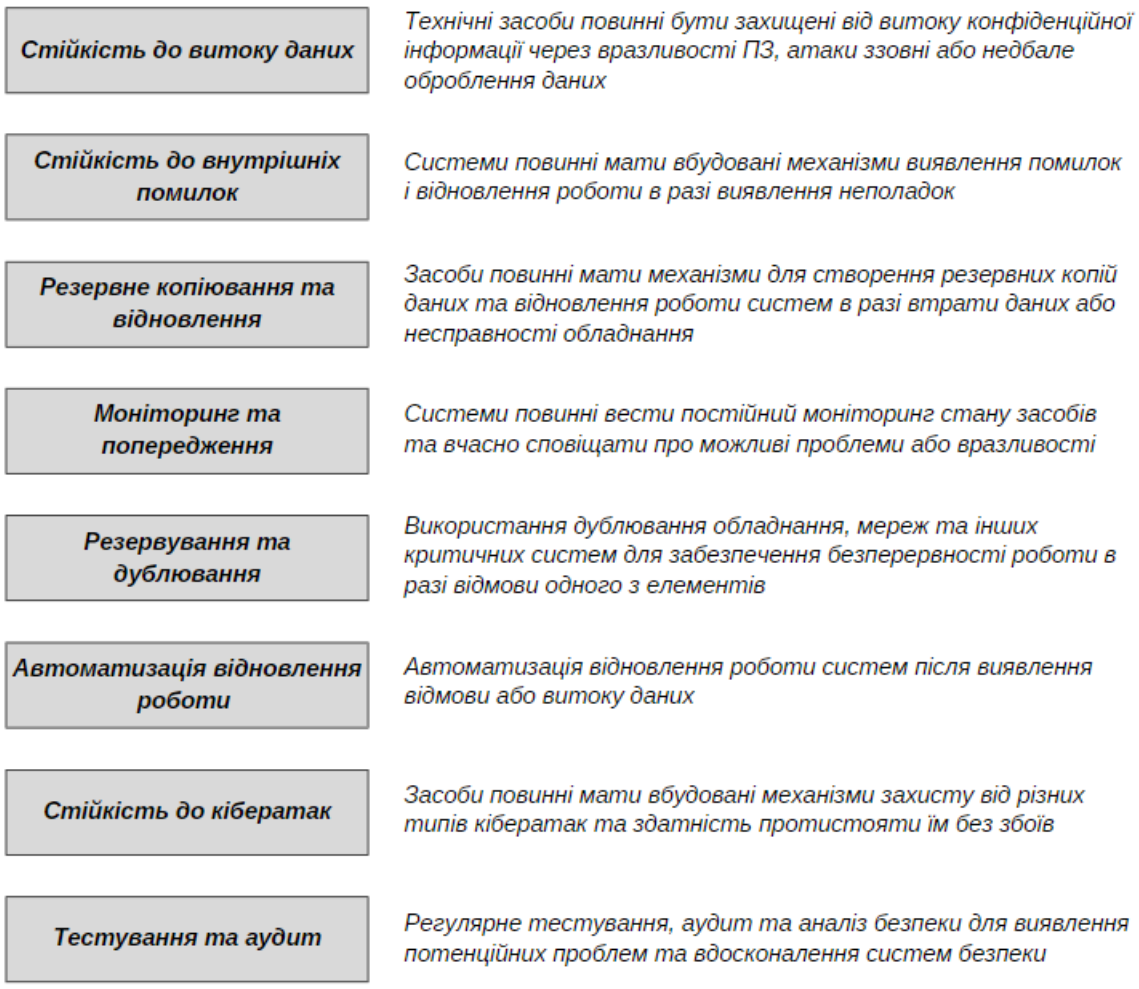


Рисунок 1.1. Важливі аспекти надійності технічних засобів

Ось деякі важливі аспекти безпеки технічних засобів:

1) захист від кібератак: технічні засоби повинні мати механізми для виявлення, блокування та відвертання різних типів кібератак, таких як DDoS, SQL ін'єкції, XSS тощо;

2) шифрування даних: засоби повинні використовувати сучасні алгоритми шифрування для захисту конфіденційної інформації в мережах, базах даних та при зберіганні даних;

3) системи виявлення та запобігання вторгнень: IDS та IPS системи допомагають виявити та зупинити вторгнення, а також захищати від зловмисних програм та шкідливого коду;

4) контроль доступу: засоби повинні забезпечувати ефективний контроль доступу до систем та ресурсів, використовуючи аутентифікацію, авторизацію та аудит;

5) захист від внутрішніх загроз: системи повинні мати механізми для виявлення та запобігання внутрішнім загрозам, таким як зловживання привілеями або недбале ставлення до безпеки;

6) моніторинг та аналіз безпеки: постійний моніторинг стану систем та вчасна реакція на підозрілу діяльність допомагають уникнути інцидентів безпеки;

7) антивірусні та антишпіонські заходи: використання антивірусного програмного забезпечення та систем захисту від шпигунського ПЗ для виявлення та усунення загроз;

8) фізична безпека: забезпечення фізичної безпеки пристроїв та інфраструктури, що включає контроль доступу, відеоспостереження та інші заходи;

9) стійкість до витоку інформації: засоби повинні мати механізми для захисту конфіденційної інформації від витоку через зовнішні атаки або внутрішні порушення.

Ці аспекти забезпечують, що технічні засоби охорони будуть надійно захищати інформацію та ресурси від різноманітних загроз, зберігаючи високий рівень безпеки та дотримання вимог до інформаційної безпеки.

Рисунок 1.2. Аспекти безпеки технічних засобів

Технічні засоби мають бути сумісними з існуючими інфраструктурами та програмним забезпеченням. Ця сумісність є критично важливою для їх успішного впровадження та ефективної роботи. Ось деякі аспекти сумісності:

1) протоколи та стандарти: технічні засоби повинні підтримувати стандартні мережеві протоколи та комунікаційні стандарти, такі як TCP/IP, HTTP, SNMP тощо;

2) інтеграція з існуючими системами: важливо, щоб нові засоби були сумісними з наявними системами, базами даних та програмами. Наприклад,

системи безпеки повинні інтегруватися з існуючими системами моніторингу або управління;

3) операційні системи: засоби повинні підтримувати операційні системи, які використовуються в організації, такі як Windows, Linux, MacOS тощо;

4) масштабованість: важливо, щоб технічні засоби могли масштабуватися разом з ростом бізнесу або потреб інфраструктури;

5) API та інтеграційні можливості: наявність API та інших інтеграційних можливостей спрощує процес інтеграції та взаємодії з іншими системами;

6) безпека: важливо, щоб нові засоби не порушували безпеку існуючої інфраструктури та програмного забезпечення і були сумісними з існуючими механізмами захисту;

7) інтерфейс користувача: інтерфейси користувача нових засобів мають бути легкими для розуміння та використання для користувачів, які вже працюють з існуючими системами;

8) вимоги щодо обладнання: засоби повинні відповідати вимогам до обладнання, щоб бути сумісними з існуючими апаратними ресурсами.

Забезпечення сумісності нових технічних засобів з існуючою інфраструктурою та програмним забезпеченням дозволяє підприємствам ефективно використовувати свої ресурси, мінімізує ризики та сприяє успішному впровадженню нових рішень.

Ефективність технічних засобів охорони є ключовим аспектом їх успішного використання. Вони повинні відповідати потребам організації та ефективно виконувати свої функції, не обмежуючи продуктивність та зручність використання. Ось кілька важливих аспектів ефективності:

1) продуктивність: технічні засоби повинні працювати швидко та ефективно, без значних затримок у виконанні своїх функцій. Наприклад, антивірусне програмне забезпечення повинно швидко сканувати систему та виявляти загрози;

2) мінімальний вплив на продуктивність: важливо, щоб використання технічних засобів не призводило до значного зниження продуктивності

користувачів або систем. Наприклад, застосування файрволу повинно не впливати на швидкість мережі;

3) низька кількість помилок: засоби повинні бути стабільними та надійними, щоб уникнути виникнення помилок та збоїв, які можуть призвести до втрати даних або недоступності систем;

4) простота використання: інтерфейси користувача повинні бути інтуїтивно зрозумілими та легкими у використанні, щоб користувачі могли швидко оволодіти функціями засобів без додаткової підготовки;

5) автоматизація: технічні засоби повинні мати можливості автоматизації для зменшення необхідності ручної участі користувачів та адміністраторів;

6) висока точність: засоби повинні точно виявляти та блокувати загрози без зайвих помилок або спрацьовувань на хибні сигнали;

7) моніторинг та звітність: засоби мають надавати зрозумілу та детальну інформацію про виявлені загрози та інциденти для адміністраторів та аналітиків безпеки;

8) скалабельність: засоби повинні бути здатні масштабуватися для відповіді на зростаючу кількість користувачів, об'єм даних або загроз;

9) оптимізація ресурсів: важливо, щоб засоби використовували ресурси (такі як обладнання, мережевий трафік тощо) ефективно та обмежено.

Рисунок 1.3. Ефективність технічних засобів охорони об’єктів

Ефективність технічних засобів охорони є критично важливою для забезпечення безпеки та продуктивності в інформаційному середовищі. Вона дозволяє організаціям ефективно використовувати свої ресурси та захищати свої інформаційні активи від різноманітних загроз.

Масштабованість технічних засобів охорони є ключовою для забезпечення їх ефективності та відповідності зростаючим потребам інформаційної безпеки. Ось деякі аспекти масштабованості:

1) горизонтальне та вертикальне масштабування: технічні засоби повинні бути здатні розширюватися горизонтально (додавання нових вузлів чи серверів) та вертикально (збільшення ресурсів на існуючих вузлах чи серверах);

2) розділення функцій: важливо, щоб функції засобів були модульними та розділені, щоб при потребі можна було додавати або змінювати певні компоненти без значного впливу на інші;

3) спільність ресурсів: засоби повинні використовувати спільні ресурси ефективно, щоб уникнути перевантаження та забезпечити стійку роботу в умовах зростаючого навантаження;

4) обробка великих обсягів даних: технічні засоби повинні бути здатні ефективно обробляти великі обсяги даних, що включає розподілену обробку, потужні алгоритми обробки даних та оптимізовані бази даних;

5) співпраця з хмарними сервісами: масштабованість може бути полегшена через інтеграцію з хмарними сервісами, які надають можливості миттєвого масштабування за потребою;

6) автоматичне масштабування: засоби повинні мати механізми автоматичного масштабування, які реагують на зростаюче навантаження та дозволяють відповідно збільшувати ресурси;

7) гнучкість: важливо, щоб засоби були гнучкими і здатними адаптуватися до різноманітних умов та потреб організації;

8) масштабування без перерв: розширення та модифікація засобів має здійснюватися без значних перерв у роботі та доступності.

9) управління масштабуванням: засоби повинні мати зручні інструменти для управління масштабуванням, що дозволяють відстежувати, контролювати та оптимізувати розширення ресурсів.

Рисунок 1.4. Складові масштабованості технічних засобів охорони

Масштабованість технічних засобів охорони дозволяє організаціям ефективно реагувати на зростаючі потреби інформаційної безпеки, забезпечуючи стабільну та ефективну роботу системи в умовах зростаючого навантаження та складності.

Простота управління та інтерфейс користувача є важливими аспектами в ефективному функціонуванні технічних засобів охорони. Вони повинні бути зрозумілими та простими для використання, щоб забезпечити ефективне управління та моніторинг системи. Ось кілька способів досягнення простоти управління:

1) інтуїтивний інтерфейс користувача: інтерфейс повинен бути логічним і легко зрозумілим для користувачів будь-якого рівня навичок. Він повинен надавати доступ до основних функцій з мінімальною кількістю клацань;

2) візуалізація інформації: використання графіків, діаграм, кольорових кодів та інших візуальних елементів для відображення інформації про стан системи;

3) мінімальна кількість кроків: максимально спрощене управління засобами захисту, можливість виконання ключових завдань з мінімальною кількістю кроків;

4) шаблони та підказки: наявність готових шаблонів налаштування та підказок, які допомагають користувачам ефективно використовувати засоби;

5) автоматизація рутинних завдань: можливість автоматизувати рутинні процеси, що дозволяє користувачам зосередитися на стратегічних аспектах безпеки;

6) підтримка мобільних пристроїв: забезпечення можливості управління системою через мобільні додатки або веб-інтерфейс, що дозволяє адміністраторам віддалено контролювати систему;

7) налаштування прав доступу: можливість налаштовувати права доступу користувачів залежно від їх ролі, що дозволяє обмежити доступ до певних функцій та інформації;

8) підтримка мов: наявність підтримки різних мов, що дозволяє користувачам з різних країн працювати з інтерфейсом на їхній власній мові;

9) навчальні матеріали та документація: наявність детальних навчальних матеріалів, посібників користувача та документації, які допомагають користувачам оволодіти засобами безпеки.

Простота управління технічними засобами охорони допомагає підвищити ефективність та зменшити ризики помилок або неправильного використання. Це дозволяє адміністраторам швидко реагувати на загрози та ефективно керувати системою безпеки.

Шифрування даних є одним з найважливіших засобів захисту конфіденційності інформації. Воно дозволяє перетворити дані у незрозумілу форму для сторонніх, що не мають необхідного ключа, тим самим захищаючи їх від несанкціонованого доступу. Ось кілька ключових аспектів шифрування даних:

1) сучасні алгоритми шифрування: засоби повинні підтримувати сучасні криптографічні алгоритми, такі як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) та інші;

2) симетричне та асиметричне шифрування: засоби можуть використовувати як симетричне, так і асиметричне шифрування. Симетричне використовує один ключ для як шифрування, так і розшифрування даних, тоді як асиметричне використовує пару ключів: публічний і приватний;

3) керування ключами: ефективне управління ключами шифрування - це важлива частина процесу. Ключі повинні зберігатися в безпечному місці і керуватися таким чином, щоб забезпечити їх конфіденційність та цілісність;

4) шифрування в спокої та в руху: засоби повинні забезпечувати шифрування як для даних, які зберігаються (наприклад, на жорстких дисках або в базах даних), так і для даних, що передаються по мережі;

5) шифрування на рівні файлів, папок, дисків: можливість шифрувати окремі файли, папки або навіть весь диск, забезпечуючи гнучкість та вибірковість захисту;

6) шифрування в хмарах: підтримка шифрування даних в хмарних сервісах, що забезпечує захист даних під час їх зберігання та передачі в хмарних середовищах;

7) висока швидкодія: засоби повинні забезпечувати швидке шифрування та розшифрування даних без помітного впливу на продуктивність системи;

8) підтримка додаткових функцій: важливо, щоб засоби мали можливість підтримувати додаткові функції, такі як цифровий підпис, аутентифікація та авторизація, які забезпечують додатковий рівень безпеки.

Шифрування даних є важливим елементом захисту конфіденційності, та забезпечує, що навіть у випадку несанкціонованого доступу до даних, вони залишаються зашифрованими та недоступними для зловмисників.

Захист від витоку інформації є критичним аспектом інформаційної безпеки. Засоби безпеки повинні забезпечувати контроль над доступом до даних і механізми для запобігання витоку конфіденційної інформації. Ось кілька ключових елементів захисту від витоку інформації:

1) управління доступом: засоби мають дозволяти адміністраторам забезпечувати контроль над тим, хто має доступ до конкретних даних та ресурсів. Це може включати різні рівні доступу для різних користувачів або груп користувачів;

2) аутентифікація і авторизація: важливо впевнитися, що лише авторизовані користувачі мають доступ до конфіденційної інформації. Це досягається шляхом ефективної аутентифікації (перевірки ідентичності користувача) і авторизації (надання прав доступу після успішної аутентифікації);

3) шифрування даних в спокої та в руху: дані повинні бути шифровані як у спокої (зберігання на серверах чи в базах даних), так і в руху (передача по мережі), щоб уникнути їх неправильного використання або перехоплення;

4) моніторинг та аудит доступу: засоби безпеки повинні вести журнали доступу, які дозволяють відстежувати, хто, коли і яким чином мав доступ до даних. Це дозволяє виявити незвичайну або підозрілу активність;

5) детектори витоку даних: засоби мають вмонтовані механізми для виявлення незвичайної активності, що може вказувати на витік інформації, такі як спроби неавторизованого доступу чи надмірний обсяг даних, що передаються з мережі;

6) контроль змін даних: важливо відстежувати та контролювати зміни в даних, особливо тих, які містять конфіденційну інформацію. Це може включати контроль версій документів або механізми блокування змін;

7) контроль відправлення даних: засоби мають можливість контролювати та обмежувати передачу конфіденційної інформації за межі організації. Це включає фільтрацію електронної пошти, веб-фільтри та інші механізми захисту від витоку даних;

8) ефективне управління політиками безпеки: організації повинні мати чіткі політики та процедури щодо обробки, зберігання та передачі конфіденційної інформації, а засоби безпеки повинні допомагати в їхньому ефективному впровадженні та дотриманні;

9) навчання персоналу: навчання користувачів та адміністраторів стосовно засобів захисту від витоку даних та їх правильного використання є важливим аспектом забезпечення безпеки.

Забезпечення захисту від витоку інформації допомагає зберегти конфіденційність, цілісність та доступність даних, забезпечуючи високий рівень безпеки для організації.

Резервне копіювання і відновлення є ключовими аспектами забезпечення безпеки даних і відновлення бізнес-процесів у разі втрати або пошкодження даних. Ось деякі важливі пункти стосовно цих механізмів:

1) регулярність копіювання: система повинна забезпечувати можливість автоматичного або ручного створення регулярних резервних копій даних з урахуванням потреб бізнесу. Це може бути щоденне, щотижневе, щомісячне або інше регулярне розкладування;

2) мінімальний час відновлення (RTO): засоби повинні дозволяти швидке відновлення даних в разі необхідності, мінімізуючи час, протягом якого бізнес не може користуватися даними;

3) мінімальність втрат даних (RPO): засоби повинні гарантувати, що втрати даних при відновленні є мінімальними. Це визначає максимальний час,

який може пройти між останньою резервною копією та моментом відмови, якого може допустити бізнес;

4) захист даних: резервні копії повинні зберігатися в безпечному місці, захищеному від фізичних пошкоджень, випадкового видалення або зловмисних атак;

5) шифрування копій: резервні копії даних повинні бути шифрованими для захисту від несанкціонованого доступу, особливо якщо вони зберігаються у віддалених місцях або в хмарних сервісах;

6) механізми відновлення: засоби повинні мати інтуїтивний і простий інтерфейс для відновлення даних, що дозволяє оперативно відновити необхідну інформацію;

7) тестування процедур відновлення: регулярні тестування процедур відновлення даних дозволяють переконатися в їхній ефективності та вчасно виявляти можливі проблеми;

8) автоматизація: засоби повинні підтримувати автоматичне виконання процесів резервного копіювання та відновлення, щоб уникнути людських помилок та забезпечити їх регулярність;

9) декомпозиція даних: резервне копіювання повинно бути декомпозовано за типами даних, пріоритетами відновлення, обсягом тощо, щоб забезпечити оптимізацію процесу відновлення.

Забезпечення ефективного резервного копіювання і відновлення даних є критичним для забезпечення безпеки і неперервності роботи бізнесу в умовах потенційних загроз та випадкових втрат даних.

Автоматизація є важливим елементом сучасних систем безпеки і дозволяє ефективно виявляти, аналізувати та реагувати на потенційні загрози. Ось деякі ключові аспекти автоматизації:

1) моніторинг та виявлення вторгнень: засоби повинні автоматично моніторити мережевий трафік, журнали подій та інші дані на предмет виявлення незвичайних або підозрілих активностей;

2) аналіз аномалій: системи повинні автоматично аналізувати дані для виявлення аномалій, що можуть вказувати на потенційні загрози або вторгнення;

3) автоматичні реакції на загрози: засоби безпеки можуть автоматично реагувати на виявлені загрози, наприклад, блокуючи підозрілий трафік, відключаючи атаковані системи або сповіщаючи адміністраторів;

4) оновлення та патчі: автоматизовані процеси оновлення дозволяють швидко встановлювати нові версії програмного забезпечення та застосовувати важливі патчі без перерв у роботі систем;

5) конфігураційне керування: автоматизоване керування конфігураціями систем дозволяє виявляти та виправляти відхилення від стандартів безпеки;

6) автоматизовані тести безпеки: системи можуть автоматично виконувати тести безпеки, такі як сканування портів, перевірку на вразливості та інші види аналізу, щоб виявити можливі ризики безпеки;

7) автоматизовані реагування на інциденти: системи можуть автоматично ініціювати заходи реагування на інциденти, наприклад, сповіщати відповідальних осіб, ізолювати збурені області мережі або навіть автоматично відновлювати системи до безпечного стану;

8) моделювання загроз: автоматизовані системи можуть моделювати потенційні загрози та атаки для ідентифікації слабких місць у системі та виявлення можливих сценаріїв атак;

9) машинне навчання та штучний інтелект: використання машинного навчання та штучного інтелекту для аналізу великих обсягів даних та виявлення складних шаблонів в активності, що вказують на загрози.

Автоматизація дозволяє забезпечити швидку реакцію на загрози, зменшити вплив людських помилок та забезпечити постійний моніторинг безпеки, що допомагає збільшити ефективність та надійність захисту інформації.

Рисунок 1.5. Ключові аспекти автоматизації ТЗО

1.1.2 Відповідність засобів охоронної сигналізації до законодавства України

Засоби охоронної сигналізації повинні відповідати вимогам законодавства України, зокрема:

– Закон України "Про охорону об'єктів інформації": засоби охоронної сигналізації повинні відповідати вимогам щодо захисту інформації, зберігання конфіденційних даних та запобігання несанкціонованому доступу до них;

– будівельний кодекс України: засоби охоронної сигналізації повинні відповідати нормам і вимогам щодо безпеки будівель та споруд;

– пожежний кодекс України: засоби охоронної сигналізації повинні відповідати вимогам щодо попередження та протидії пожежам, зокрема, виявлення пожежі та вчасного сповіщення про неї;

– Закон України "Про телекомунікації": засоби охоронної сигналізації, які використовують комунікаційні засоби, повинні відповідати вимогам щодо використання радіочастот та інших засобів зв'язку;

– правила експлуатації систем охоронної сигналізації: цей документ містить вимоги до встановлення, налаштування, експлуатації та обслуговування систем охоронної сигналізації;

– нормативно-технічні вимоги ДСТУ: це стандарти та вимоги до якості та безпеки обладнання, які використовуються в системах охоронної сигналізації;

– вимоги Держпромгірнагляду: відповідно до вимог Держпромгірнагляду, системи охоронної сигналізації повинні відповідати встановленим стандартам і бути сертифіковані;

– вимоги до персоналу та організації роботи: організації, які встановлюють і обслуговують системи охоронної сигналізації, повинні мати кваліфікований персонал та дотримуватися вимог до їх роботи.

Всі ці вимоги спрямовані на забезпечення ефективної та безпечної роботи систем охоронної сигналізації для захисту об'єктів та майна в Україні.

Відповідність до вимог законодавства та стандартів є критично важливою для забезпечення безпеки та конфіденційності інформації. Ось кілька важливих аспектів:

– GDPR (Загальний регламент про захист даних): засоби повинні забезпечувати виконання вимог GDPR, таких як право на забування, обмеження обробки даних, надання доступу до даних, повідомлення про порушення безпеки тощо;

– HIPAA (Закон про портативність та захист медичних даних): системи повинні відповідати вимогам HIPAA щодо захисту конфіденційності та безпеки медичної інформації, включаючи заходи для обмеження доступу до даних, аудит доступу, шифрування тощо;

– ISO 27001 (Міжнародний стандарт з інформаційної безпеки): засоби безпеки повинні відповідати вимогам ISO 27001, забезпечуючи ефективне управління ризиками, виявлення та захист від загроз, а також систематичну перевірку та вдосконалення систем безпеки;

– PCI DSS (Стандарт безпеки платіжних карт): якщо системи обробляють платіжну інформацію, вони повинні відповідати вимогам PCI DSS, що

включають захист від несанкціонованого доступу, шифрування даних, виконання тестів на вразливість тощо;

– секторні стандарти та регулювання: в залежності від сектору діяльності (фінансовий, медичний, державний тощо) можуть бути встановлені додаткові вимоги та стандарти, які також повинні бути враховані;

– аудит та звітність: засоби безпеки повинні забезпечити можливість проведення аудитів та створення звітів про відповідність вимогам законодавства та стандартів;

– наявність документації та політик безпеки: важливо, щоб засоби мали можливість документувати політики безпеки, процедури та заходи, що вживаються для відповідності вимогам;

– регулярне оновлення: засоби повинні бути оновлюваними та адаптованими до змін в законодавстві та стандартах безпеки.

Забезпечення відповідності до вимог законодавства та стандартів є важливим для будь-якої організації, оскільки дозволяє уникнути штрафів, зберегти довіру клієнтів тощо.

1.1.3 Складові технічних засобів охорони

Технічні засоби охорони включають різні складові, які спільно допомагають забезпечити безпеку об'єкта чи території. Основні складові технічних засобів охорони включають: відеоспостереження; системи контролю доступу; сигналізація та виявлення вторгнень; контроль доступу до мережі інформації; системи виявлення пожежі та безпеки; відеоінтерком та системи огляду; технології ідентифікації та трекінгу.

Ці складові можуть використовуватися окремо або спільно для створення комплексної системи безпеки, яка відповідає потребам конкретного об'єкта чи території.

Відеоспостереження – це одна з найпоширеніших технологій безпеки. Система відеоспостереження включає в себе використання відеокамер, які відстежують діяльність на об'єкті або визначені області. Сучасні системи можуть

мати високу роздільну здатність, можливість запису, аналізу відео та функції розпізнавання обличчя.

Відеоспостереження дійсно є однією з найпоширеніших та найефективніших технологій безпеки. Ось кілька ключових компонентів і можливостей сучасних систем відеоспостереження:

1) відеокамери – це основний елемент системи, який зафіксовує відеоінформацію. Сучасні відеокамери можуть мати високу роздільну здатність (HD, Full HD, 4K), а також можуть бути обладнані функціями нічного бачення, автоматичного фокусування, регулювання яскравості тощо;

2) монітори та запис: відеосигнал з камер може бути відображений на моніторах для реального часу спостереження або записаний на носії інформації для подальшого аналізу чи зберігання. Сучасні системи можуть мати вбудований жорсткий диск або використовувати хмарне зберігання;

3) аналіз відео та розпізнавання обличчя: деякі системи відеоспостереження мають функції аналізу відео, які дозволяють виявляти певні події (наприклад, рух) або вести відслідковування об'єктів. Розпізнавання обличчя дозволяє ідентифікувати людей на відеозаписах;

4) мережеве підключення: багато сучасних систем відеоспостереження підтримують мережеве підключення, що дозволяє віддалене спостереження через Інтернет з будь-якої точки світу за допомогою смартфонів, планшетів або комп'ютерів;

5) інтеграція з іншими системами безпеки: відеоспостереження може бути інтегровано з іншими системами безпеки, такими як системи контролю доступу, сигналізації та виявлення вторгнень, для створення комплексної системи безпеки;

6) інфрачервоне та теплове відеоспостереження: такі системи дозволяють виявляти об'єкти в темряві або в умовах обмеженої видимості, що робить їх ефективними вночі або в умовах поганих погодних умов.

Використання сучасних технологій у системах відеоспостереження значно підвищує рівень безпеки та дозволяє ефективно відстежувати та реагувати на потенційні загрози.

Системи контролю доступу дозволяють регулювати доступ до об'єкта чи приміщення. Вони включають в себе електронні замки, картки доступу, біометричні ідентифікатори (відбитки пальців, розпізнавання облич), а також системи персонального кодування.

Системи контролю доступу грають важливу роль у забезпеченні безпеки об'єктів та приміщень. Ось деякі основні компоненти і можливості таких систем:

1) електронні замки замінюють традиційні механічні замки та контролюють доступ до дверей, воріт або інших точок входу. Вони можуть бути керовані з центральної системи або місцево з допомогою картки, коду чи біометричних даних;

2) картки доступу – це електронні картки або ключі, які авторизують особу на доступ до об'єкта. Картки можуть бути зчитуваними з магнітною смугою, RFID-чипом або бездротовим зв'язком;

3) системи біометричної ідентифікації використовують біометричні дані, такі як відбитки пальців, розпізнавання облич чи розпізнавання радужки ока, для ідентифікації особи. Вони надають високий рівень безпеки, оскільки біометричні дані унікальні для кожної особи;

4) системи персонального кодування вимагають введення особистого коду доступу або PIN-коду для розблокування двері. Код може бути введений на клавіатурі або сенсорному екрані;

5) централізоване управління: багато систем контролю доступу мають централізовану систему управління, яка дозволяє адміністраторам налаштовувати права доступу, відстежувати активність користувачів та керувати системою в цілому;

6) аудит доступу: ця функція дозволяє вести журнал подій, в якому фіксується інформація про всі події, пов'язані зі зміною доступу, такі як час входу/виходу, використані картки чи біометричні дані;

7) дистанційне керування: деякі системи дозволяють віддалено керувати доступом через Інтернет або мобільний додаток, що дозволяє адміністраторам встановлювати права доступу або надавати тимчасовий доступ.

Ці складові дозволяють створювати ефективні системи контролю доступу, які забезпечують високий рівень безпеки та контролю над доступом до об'єктів.

Сигналізація та виявлення вторгнень: ці системи виявляють незаконний доступ або порушення на об'єкті. Вони можуть включати в себе датчики руху, датчики відкриття, датчики скляних боєвих систем (розбиття скла), а також акустичні або оптичні сигналізатори.

Системи сигналізації та виявлення вторгнень є ключовими у забезпеченні безпеки об'єктів. Ось деякі основні компоненти цих систем:

1) датчики руху реагують на рух в певній зоні і сприймають зміни в інфрачервоному випромінюванні, мікрохвилях або звуку. Датчики можуть бути розташовані вздовж стін або в певних точках, де найімовірніше вторгнення;

2) датчики відкриття виявляють відкриття дверей, вікон або інших доступних точок. Вони можуть використовувати магнітні контакти, оптичні сенсори або механічні вимикачі;

3) датчики скляних боєвих систем реагують на розбиття скла і відкривають тривожну сигналізацію. Вони можуть бути розміщені на вікнах або скляних дверях;

4) акустичні або оптичні сигналізатори виробляють гучний звук або світлові сигнали, щоб попередити про вторгнення або активувати внутрішню сирену для виклику допомоги;

5) системи відеоспостереження можуть бути інтегровані з системами сигналізації, щоб відслідковувати події, які призвели до активації тривожної сигналізації, і надсилати відеозаписи на контрольний центр або мобільний пристрій;

6) мережеве підключення системи сигналізації підтримують мережеве підключення, що дозволяє надсилати сповіщення адміністраторам чи власникам об'єкта через Інтернет;

7) централізоване керування: в центрі системи є пульт керування, де адміністратор може моніторити статус системи, отримувати тривожні сповіщення та вживати заходів у разі необхідності;

8) безпровідна технологія використовує бездротові технології для зв'язку між датчиками та центральним блоком, що дозволяє швидку та просту інсталяцію.

Ці компоненти дозволяють системам сигналізації та виявлення вторгнень ефективно виявляти та реагувати на потенційні загрози для безпеки об'єкта.

Контроль доступу до мережі інформації – це критичний аспект забезпечення безпеки в сучасних організаціях. Ось деякі ключові компоненти цих систем:

1) файерволи (Firewalls) – ці системи контролюють трафік, який входить та виходить з мережі, застерігаючи від несанкціонованого доступу та захищаючи мережеві ресурси від зловмисників. Вони можуть бути апаратними або програмними, здатними аналізувати пакети даних та виконувати правила безпеки;

2) системи виявлення вторгнень (IDS/IPS) – ці системи моніторять мережу на виявлення аномальних або підозрілих активностей. IDS аналізує трафік на предмет зловмисних дій, тоді як IPS може блокувати або відхиляти шкідливий трафік;

3) антивірусне програмне забезпечення призначено для виявлення, блокування та видалення шкідливого програмного забезпечення, такого як віруси, черви, троянці та інші загрози;

4) віртуальні приватні мережі (VPN): VPN створюють зашифроване з'єднання між комп'ютерами чи мережами через публічну мережу, таку як Інтернет. Вони забезпечують конфіденційність та цілісність даних під час передачі через небезпечні середовища;

5) методи аутентифікації включають у себе різні методи перевірки ідентичності користувачів перед наданням доступу до мережі, такі як паролі,

біометричні дані (відбитки пальців, розпізнавання облич), токени або двофакторна аутентифікація;

6) шифрування даних дозволяє захищати конфіденційні дані під час їх транспортування по мережі. Воно може застосовуватися як на рівні мережі, так і на рівні даних;

7) моніторинг та аналіз мережі – ці системи виявляють потенційні загрози та вразливості в мережі шляхом аналізу трафіку, аудиту подій та іншими методами.

Ці компоненти допомагають створити комплексні системи контролю доступу до мережі інформації, які забезпечують високий рівень безпеки та захисту даних.

Системи виявлення пожежі та безпеки: ці системи виявляють пожежу, дим або інші загрози безпеки та ініціюють відповідні заходи. Вони можуть включати в себе димові детектори, детектори температури, системи виявлення газів, автоматичні спринклерні системи та інші.

Такі системи грають важливу роль у запобіганні пожеж та інших аварійних ситуацій. Ось деякі основні компоненти таких систем:

1) димові детектори – ці пристрої реагують на наявність диму в приміщенні. Вони можуть бути оптичними (спираються на розсіювання світла), іонізуючими (виявляють іони, які утворюються під час горіння) або комбінованими;

2) детектори температури – ці пристрої виявляють зміни температури, що можуть вказувати на пожежу. Вони можуть мати фіксовані температурні пороги або бути програмованими для виявлення швидких змін температури;

3) системи виявлення газів виявляють наявність небезпечних газів, таких як димонабірні гази, вуглекислий газ, метан тощо. Ці системи можуть виявляти гази шляхом аналізу концентрації в повітрі або детекторами хімічних речовин;

4) автоматичні спринклерні системи – ці системи автоматично активуються при виявленні пожежі та починають розпилення води або іншого вогнегасного середовища для гасіння пожежі або обмеження її поширення;

5) тривожні сигналізатори – системи виявлення пожежі також можуть включати в себе тривожні сигналізатори, які сповіщають людей на об'єкті про небезпеку і вказують місце, де виникла пожежа;

6) системи автоматичного виклику пожежної служби автоматично надсилають сигнал про пожежу на пожежну станцію, щоб оперативно реагувати на небезпеку;

7) відеоспостереження: відеокамери можуть бути інтегровані в системи виявлення пожежі для відстеження подій та допомоги у виявленні джерела пожежі.

Ці компоненти дозволяють створити надійні системи виявлення пожежі та безпеки, які реагують на загрози негайно і ефективно, забезпечуючи безпеку приміщень та мешканців.

Відеоінтерком та системи огляду дозволяють взаємодіяти зі вхідними або зовнішніми відвідувачами, переглядати їх, спілкуватися та контролювати доступ. Вони можуть включати в себе відеоінтеркоми, системи відеоогляду та домофони.

Відеоінтерком та системи огляду – це важливі компоненти систем безпеки та контролю доступу. Ось деякі ключові елементи цих систем:

1) відеоінтеркоми – ці системи дозволяють спілкуватися з відвідувачами, які стоять перед входом або воротами. Вони зазвичай мають камеру та динамік-мікрофон, що дозволяє вам бачити та слухати відвідувачів і комунікувати з ними в реальному часі;

2) системи відеоспостереження дозволяють спостерігати за об'єктом або територією за допомогою відеокамер. Вони можуть бути розташовані всередині та зовні будівлі для відстеження подій та дій на місці;

3) домофони дозволяють комунікувати з відвідувачами, які стоять перед вхідними дверима вашого будинку або квартири. Вони можуть мати кнопку для відкриття дверей або воріт здалеку;

4) інтерком-системи для офісів та промислових об'єктів можуть використовуватися для спілкування між різними зонами або відділами об'єкту без потреби фізичної зустрічі;

5) IP-інтеркоми та системи відеоогляду: деякі сучасні системи можуть працювати через Інтернет, що дозволяє вам спостерігати за об'єктом або спілкуватися з відвідувачами віддалено через мобільні додатки або веб-портали;

6) системи запису можуть записувати відео або аудіофайли, щоб забезпечити докази або стежити за подіями, що відбуваються під час вашої відсутності;

7) інтеграція з іншими системами – ці системи можуть бути інтегровані з іншими системами безпеки, такими як системи контролю доступу або відеоспостереження, щоб створити комплексну систему безпеки.

Ці компоненти дозволяють створити ефективні системи безпеки та контролю доступу, які забезпечують комунікацію з відвідувачами та контроль над доступом до об'єкту.

Технології ідентифікації та трекінгу: ці системи дозволяють визначати та відстежувати об'єкти або особи. Вони можуть використовувати RFID-мітки, GPS-трекери, системи радіочастотної ідентифікації (RFID), а також інші технології.

Точно, технології ідентифікації та трекінгу дозволяють визначати та відстежувати об'єкти або особи в реальному часі. Ось деякі ключові технології:

1) RFID (Radio Frequency Identification) – ця технологія використовує радіочастотні мітки для ідентифікації та відстеження об'єктів. Мітки мають унікальний ідентифікатор, який може бути зчитаний за допомогою RFID-считувача. Вона застосовується в різних галузях, від логістики до безпеки;

2) GPS (Global Positioning System) трекери – ці пристрої використовують сигнали з супутників для визначення місця розташування об'єкта. Вони широко використовуються в автомобільній промисловості, логістиці, а також для відстеження руху осіб чи тварин;

3) системи радіочастотної ідентифікації (RFID) використовують радіочастоту для спілкування між мітками та зчитувачами. Ці системи застосовуються в контролі доступу, логістиці, виробництві та інших галузях;

4) біометричні системи ідентифікації – використовують біологічні або поведінкові характеристики, такі як відбитки пальців, розпізнавання облич, сканування радужки ока чи голосові відомості, для ідентифікації осіб. Ці системи широко застосовуються в сферах безпеки, відправлення та управління доступом;

5) бездротові мережі та маяки використовуються для визначення місця розташування об'єктів або осіб у певному радіусі дії. Ці технології дозволяють визначити місце розташування в реальному часі та встановити відповідні дії;

6) QR-коди та штрих-коди можуть бути використані для ідентифікації товарів, документів чи об'єктів. Вони широко використовуються в роздрібній торгівлі, логістиці та управлінні запасами;

7) технології відстеження за допомогою камер: деякі системи відеоспостереження можуть використовувати комп'ютерний зір для відстеження руху та ідентифікації об'єктів на відеозаписах.

Ці технології дозволяють відстежувати об'єкти або особи в реальному часі та виконувати різноманітні завдання, від логістики до безпеки.

1.2 Аналіз принципів роботи датчиків сигналізації

1.2.1 Типи датчиків охоронної сигналізації

Датчики охоронної сигналізації грають важливу роль у виявленні небажаних подій, таких як вторгнення, пожежі або витоки газу. Основні принципи їх роботи можуть варіювати залежно від типу датчика, але загальною метою є виявлення небезпечних або небажаних ситуацій і сповіщення власника про них. Ось деякі загальні принципи роботи різних типів датчиків охоронної сигналізації:

1) датчики руху (PIR):

- вони виявляють рух за допомогою інфрачервоних сенсорів;

- коли об'єкт проходить через поле зору датчика, він змінює температуру, і це сприймається сенсорами;

- сигнал про рух активує сигналізаційну систему;

2) магнітні датчики (дверні/віконні):

- вони працюють на основі магнітного поля.;

- датчик складається з двох частин: магнітної і датчика. При відкритті дверей чи вікон ці частини втрачають взаємодію, що активує сигналізацію;

3) датчики диму:

- вони реагують на наявність диму в повітрі;

- датчики можуть бути оптичними (виявляють розсіяне світло від частинок диму) або іонізуючими (виявляють іони, що утворюються при горінні);

4) датчики вуглекислого газу (CO):

- вони реагують на підвищення рівня CO в повітрі;

- зазвичай вони мають електрохімічні сенсори, які реагують на CO;

5) датчики протікання води:

- вони реагують на наявність води або вологи;

- датчики можуть мати контактні пластики, які замикатимуть контакти при змочуванні або вологій середовища, або електричні сенсори, які реагують на зміни у провідності;

6) датчики склушування (глухоствола):

- вони реагують на звукові хвилі;

- при виявленні певного рівня звуку вони активуються;

7) датчики вибухонебезпечних речовин:

- вони реагують на викиди вибухонебезпечних речовин;

- використовують різні технології, включаючи детектори газів та хімічні датчики.

Кожен з цих типів датчиків має свої переваги та обмеження. Для оптимальної захисту зазвичай використовується комбінація датчиків різних

типів, щоб забезпечити найкращий охоплення та надійність сигналізаційної системи.

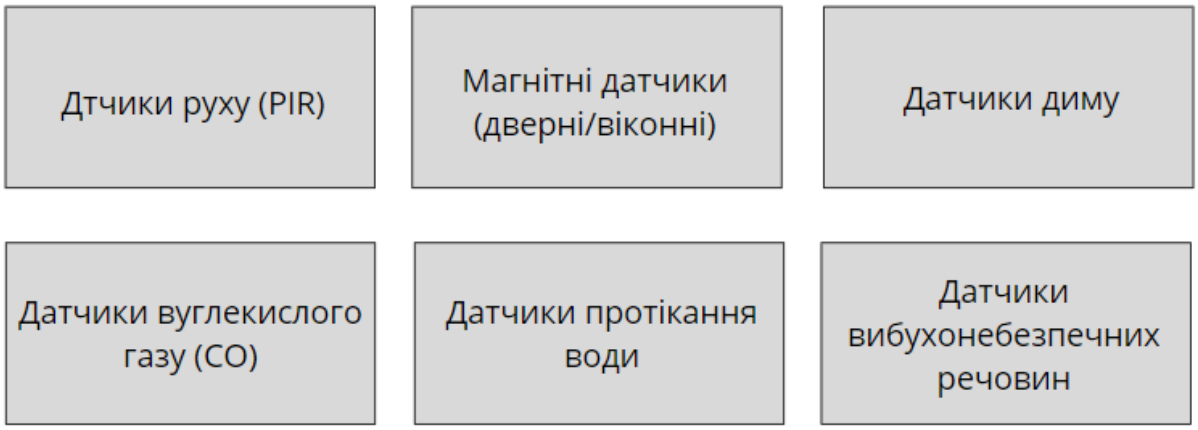


Рисунок 1.6. Базові датчики в системах охоронної сигналізації

1.2.2 Фізичні принципи дії датчиків руху

Датчики руху (PIR) виявляють рух за допомогою інфрачервоних сенсорів: коли об'єкт проходить через поле зору датчика, він змінює температуру, і це сприймається сенсорами.

Розглянемо принцип роботи датчиків руху (PIR) більш детально:

1) інфрачервоні сенсори: датчики PIR виявляють рух шляхом реагування на зміни в інфрачервоному спектрі; ці датчики використовуються для вимірювання інфрачервоного випромінювання, яке випромінюється живими і неживими об'єктами;

2) зміна температури: коли об'єкт (наприклад, людина чи тварина) проходить через поле зору датчика, він змінює температуру навколишнього середовища; температурні зміни створюють градієнт температур, який датчик може виявити;

3) детектори руху: PIR-датчики мають два або більше детектори, спрямовані в різних напрямках; коли об'єкт пересувається, він перетинає конусні зони виявлення кожного детектора, що створює зміну сигналу;

4) аналіз сигналу: сигнал, отриманий від датчиків, проходить через аналізатор, який виявляє патерни та зміни в інфрачервоному випромінюванні;

якщо аналізатор виявляє відмінності в інфрачервоному спектрі, які вказують на рух, то генерується сигнал;

5) активація сигналізації: коли виявляється рух, датчик активує сигналізаційну систему, що може включати в себе дзвінки, світлові сигнали або сповіщення до центральної системи безпеки; таке сповіщення дає можливість власнику або охоронній службі вчасно реагувати на можливу загрозу.

Датчики руху (PIR) є ефективними для виявлення руху в зоні покриття, що робить їх дуже корисними для систем безпеки та автоматичного освітлення.

На рис. 1.7 представлено зображення датчика руху.

Рисунок 1.7. Зображення датчика руху

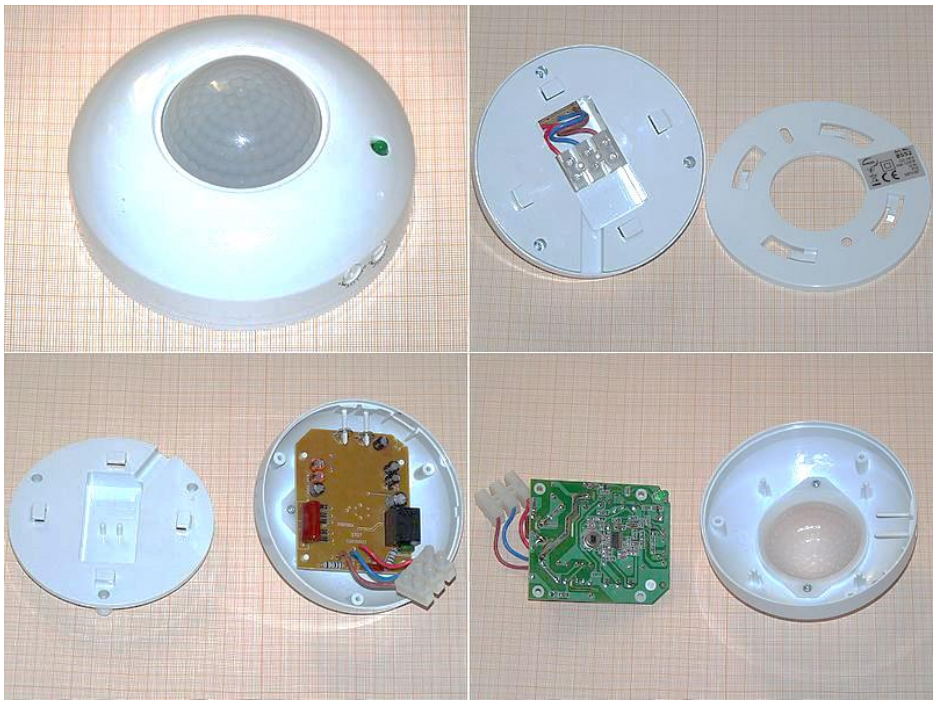


Рисунок 1.8 Інфрачервоний датчик руху

Зображення елементів інфрачервоних датчиків надано на рис. 1.9.

Рисунок 1.9. Корпуси інфрачервоних датчиків

1.2.3 Принцип дії магнітних датчиків дверей та вікон

Магнітні датчики дверей або вікон працюють за простою, але ефективною принциповою схемою. Ось як це працює:

1) основний принцип: магнітні датчики базуються на взаємодії магнітних полів;

2) складові датчика:

- магнітна частина: це постійний магніт або магнітний елемент, який прикріплюється до однієї сторони дверей або вікна;

- датчик: це датчик здатний виявляти зміни в магнітному полі. Він розташовується поруч з магнітною частиною, зазвичай на рамі або фіксується на нерухомій частині дверей або вікна;

3) принцип роботи:

- коли двері або вікно зачинені, магнітна частина тісно прилягає до датчика, створюючи магнітне поле, яке реєструється датчиком;

- при відкритті дверей або вікна магнітна частина віддаляється від датчика, руйнуючи магнітне поле;

- ця зміна в магнітному полі активує датчик, і як результат, спрацьовує сигналізаційна система;

4) активація сигналізації:

- після того, як датчик виявить віддалення магнітної частини, він надсилає сигнал до системи сигналізації;

- система сигналізації, будь то домашня або комерційна, активується, сповіщаючи власника про відкриття дверей або вікон;

5) варіації:

- існують різні типи магнітних датчиків, такі як поверхневі, вбудовані, радіочастотні тощо, залежно від конкретних потреб і умов встановлення.

Магнітні датчики дверей і вікон - це надійний і простий спосіб захисту будинку або будь-якого іншого приміщення від несанкціонованого входу.

На рис. 1.10 – 1.11 надано зображення магнітних датчиків (герконовий датчик).

Рисунок 1.10. Зображення магнітного датчика вікна

Рисунок 1.11. Магнітоконтактний датчик Електрон СМК-7ЭП

1.2.4 Датчики диму

Датчики диму є важливою складовою будь-якої системи пожежного сповіщення і безпеки. Ось як вони працюють:

1) основний принцип: датчики диму реагують на наявність диму в повітрі.

2) типи датчиків:

- оптичні датчики:

- вони виявляють розсіяне світло, яке утворюється внаслідок попадання частинок диму у світловий промінь, який поступає від світлодіода або іншого світлового джерела;

- коли дим попадає в промінь світла, він розсіює його, змінюючи інтенсивність світла, яке потрапляє на фотодетектор. Ця зміна інтенсивності спрацьовує датчик;

- іонізуючі датчики:

- вони виявляють іони, які утворюються при горінні.

- при горінні матеріалу, такого як дерево або пластик, утворюються іони, які стають провідними для струму;

- датчик містить два електроди та джерело радіації. Іони, що утворюються в диму, змінюють провідність між електродами, спричиняючи спрацьовування датчика;

3) принцип роботи:

- при наявності диму, який включає частинки, оптичний датчик виявляє зміни в розсіяному світлі;

- у випадку іонізуючого датчика, коли дим утворює іони, провідність повітря змінюється, що викликає реакцію датчика;

- після того, як датчик виявляє присутність диму, він активує систему пожежного сповіщення;

4) активація системи пожежного сповіщення:

- коли датчик диму спрацьовує, він відправляє сигнал до центрального блоку пожежної сигналізації;

- центральний блок активує сповіщення, такі як сирени, миготливі вогнеборці або автоматичне сповіщення служб пожежної охорони.

5) варіації:

- існують інші типи датчиків диму, такі як теплові датчики, які реагують на збільшення температури, а не на дим.

Датчики диму є критичним елементом системи пожежного сповіщення і безпеки, допомагаючи рано виявляти пожежі і запобігати поширенню вогню.

1.2.5 Датчики вуглекислого газу

Датчики вуглекислого газу (CO) є важливою складовою системи безпеки в будь-якому приміщенні, особливо в домашніх умовах. Ось як вони працюють:

1) основний принцип: датчики CO реагують на підвищення рівня CO в повітрі, що може бути небезпечним для здоров'я та життя людей;

2) типи датчиків:

- електрохімічні сенсори:

- ці сенсори містять електроди, покриті хімічною реакцією, яка відбувається при контакті з CO;

- коли CO взаємодіє з електродами, відбувається хімічна реакція, яка змінює електричний струм у датчику;

- зміна електричного струму спрацьовує датчик, сигналізуючи про наявність CO в повітрі;

3) принцип роботи:

- коли рівень CO в повітрі підвищується, молекули CO взаємодіють з електрохімічними сенсорами;

- ця взаємодія спричиняє зміну потенціалу на електродах, що призводить до зміни струму, що проходить через сенсор;

- зміна струму активує датчик, сигналізуючи про наявність CO в повітрі.

4) активація сигналізації:

- після того, як датчик виявляє підвищений рівень CO, він надсилає сигнал до системи пожежного сповіщення або димовидаляючої системи;

- система активує сигналізацію, яка може включати сирени, миготливі світлові сигнали, а також відправку сповіщення на мобільний телефон власника або службу безпеки;

5) варіації: існують різні типи датчиків CO, такі як портативні, які можна переносити з собою, і стаціонарні, які встановлюються на певних місцях у приміщенні.

Датчики вуглекислого газу є важливими для запобігання отруєння CO, особливо в приміщеннях з газовими опалювальними системами або поблизу

гаражів. Вони допомагають вчасно виявити небезпеку і запобігти отруєнню або пожежі.

1.2.6 Датчики протікання води

Датчики протікання води є важливими для виявлення витоків та запобігання затопленням. Ось як вони працюють:

1) основний принцип: датчики протікання води реагують на наявність води або вологи в певній області;

2) типи датчиків:

- контактні пластики:

- ці датчики містять два контактних елементи, які не замкнені один на одного, коли середовище сухе;

- при попаданні води або вологи контактні пластики замикують контакти, що створює електричне замикання;

- електричні сенсори:

- вони реагують на зміни у провідності в середовищі в результаті змочування або вологи;

- зазвичай вони містять два електроди, які змінюють провідність між собою, коли є вода або волога;

3) принцип роботи:

- при наявності води або вологи, контактні пластики замикатимуть контакти або електричні сенсори змінятимуть свою провідність;

- ця зміна електричного стану активує датчик, сигналізуючи про наявність вологи;

4) активація сигналізації:

- після того, як датчик виявить протікання води, він надсилає сигнал до системи попередження або аварійної сигналізації;

- система може включати автоматичне відключення водопостачання, сповіщення власника будинку через смс або додаток, а також сигналізацію звукових або візуальних сигналів;

5) варіації:

- існують різні типи датчиків протікання води, такі як датчики для підлоги, датчики для пристроїв і трубопроводів, а також портативні датчики для використання в окремих приміщеннях або пристроях.

Датчики протікання води допомагають вчасно виявляти витоки та запобігати серйозним затопленням, що може призвести до знищення майна або навіть загрози для безпеки

1.3 Розробка системи охоронної сигналізації підприємства

1.3.1 Початкові дані для розробки системи ОС підприємства

Розглянемо наступне завдання для розробки системи охоронної сигналізації підприємства, яке складається з наступних підрозділів:

1) кімната директора;

2) кімната секретарка:

3) кімната бухгалтера;

4) кімната відділу збуту та постачання;

5) кімната відділу постачання;

6) санітарна кімната;

7) хол.

Потрібно побудувати комплексну систему охоронної сигналізації підприємства таким чином, щоб уникнути проникнення в приміщення порушника без спрацювання сигналізації. Також потрібно забезпечити можливість гнучкого налаштування параметрів системи.

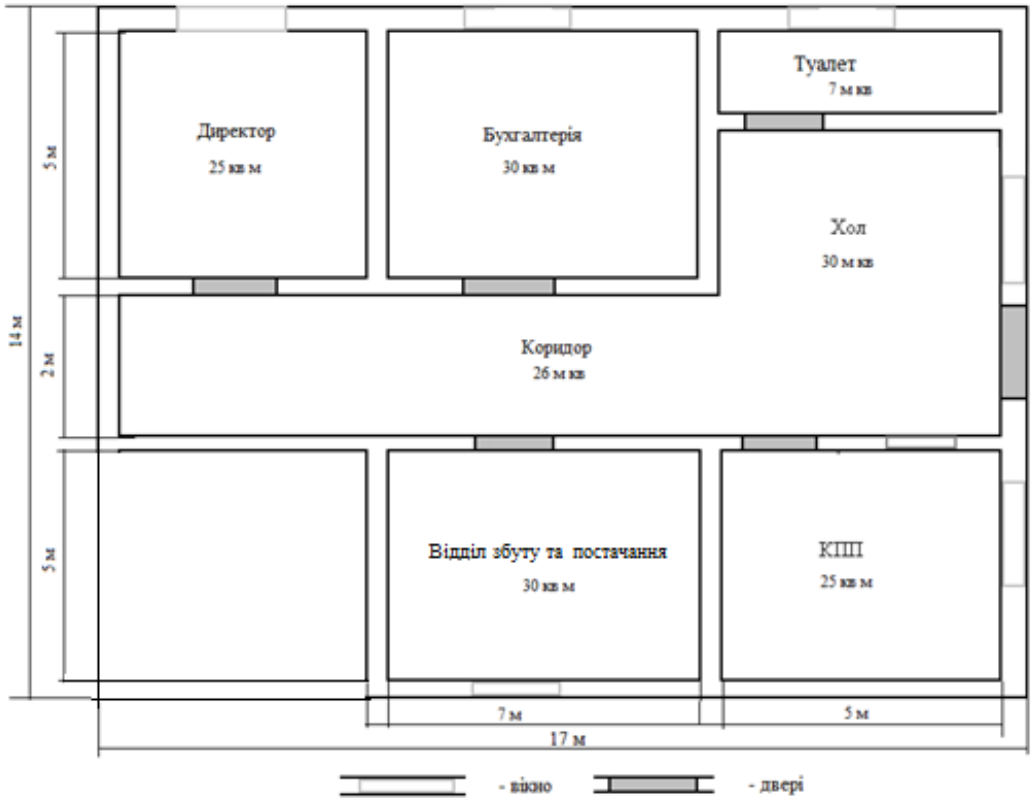


Рисунок 1.12. План підприємства

1.3.2 Обґрунтування вибору платформи Arduino для розробки системи охоронної сигналізації підприємства

Обираючи платформу Arduino, можна виходити з кількох важливих обґрунтувань:

1) простота використання: Arduino - це одна з найпопулярніших платформ для початківців і професіоналів. Її простота використання полягає в зручності програмування (на мові C/C++), доступності багатьох бібліотек і готових рішень для різних типів датчиків та пристроїв;

2) велике спільнота і підтримка: Arduino має велику активну спільноту користувачів, що дозволяє швидко знайти відповіді на будь-які питання та проблеми, а також отримати поради з розробки проектів;

3) наявність готових модулів і датчиків: на ринку існує велика кількість готових модулів, сенсорів та розширювачів для платформи Arduino, що значно спрощує розробку електронних пристроїв та прототипів;

4) низька вартість: Arduino платформа і самі плати досить доступні в ціновому плані порівняно з іншими мікроконтролерами і платформами для вбудованих систем;

5) великий вибір моделей: Arduino пропонує різні моделі мікроконтролерів для різних завдань, включаючи більш потужні версії для складніших проектів та менш потужні для економії енергії;

6) широкий спектр застосувань: Arduino може використовуватися для розробки різних типів проектів, від простих світлодіодних лампочок до складних систем автоматизації та IoT пристроїв.

Загалом, Arduino – це дуже зручна, доступна та масова платформа для розробки різноманітних електронних проектів.

Обґрунтування вибору мікроконтролера Arduino UNO також базується на кількох важливих аспектах:

1) популярність та доступність: Arduino UNO – одна з найпопулярніших моделей мікроконтролерів. Її можна легко придбати в магазинах електроніки, і вона доступна для широкого кола користувачів;

2) простота використання: Arduino UNO має простий для розуміння і використання інтерфейс, що робить його ідеальним для початківців та студентів. Крім того, для нього доступно безліч навчальних матеріалів та підручників;

3) гнучкість: Arduino UNO має достатньо ресурсів (пам'ять, введення-виведення тощо), щоб реалізувати багато різних проектів, від простих LED-маяків до складніших IoT систем;

4) велика кількість портів вводу-виводу (I/O): Arduino UNO має достатньо цифрових і аналогових входів та виходів для підключення до нього різноманітних сенсорів, пристроїв та модулів;

5) сумісність з різними модулями та сенсорами: через велику популярність Arduino UNO на ринку існують сотні сумісних модулів, сенсорів та розширювачів, що робить його дуже гнучким для реалізації різноманітних ідей;

6) підтримка спільноти: через широку популярність, у вас завжди є можливість звернутися до спільноти з питаннями та отримати відповіді або поради;

7) вартість: Arduino UNO – досить доступний з точки зору ціни мікроконтролер, що дозволяє економити кошти при реалізації проектів.

Отже, мікроконтролер Arduino UNO є відмінним вибором для багатьох проектів завдяки своїй простоті використання, гнучкості та доступності.

На рис 3.2 надано зображення плати мікроконтролера Arduino UNO.

Рисунок 1.13. Зображення плати мікроконтролера Arduino UNO

Ось основні параметри плати мікроконтролера Arduino UNO:

1) мікроконтролер - ATmega328P;

2) робоча вхідна напруга від 5V до 12V;

3) рекомендована напруга живлення від 7V до 12V. Максимальна напруга - 6V-20V;

4) цифрові входи/виходи (GPIO): 14 цифрових входів/виходів, з яких 6 можуть використовуватися для генерації шириною імпульсів модульного сигналу (PWM);

5) аналогові входи: 6 аналогових входів з 10-бітним роздільною здатністю;

6) швидкість процесора: 16 MHz;

7) оперативна пам'ять (RAM): 2 KB;

8) пам'ять програми (Flash): 32 KB (включаючи 0.5 KB використовувані для заголовків загрузки);

9) EEPROM: 1 KB;

10) термінали з'єднання:

- USB: для програмування та живлення;
- DC живлення: для зовнішнього живлення плати;
- Vin: вхідна напруга для живлення від DC або AC адаптера;

11) розміри плати: 68.6 мм на 53.4 мм;

12) інтерфейс USB для з'єднання з комп'ютером для програмування та зчитування/запису програм;

13) кварцовий резонатор: 16 MHz;

14) LED-індикатори: є вбудовані LED-індикатори для вказівки статусу живлення та активності (RX, TX);

15) тип інтерфейсу: Serial, SPI, I2C.

Ці параметри роблять Arduino UNO досить потужною та гнучкою платформою для розробки різних електронних проектів.

1.3.3 Розробка системи схеми охоронної системи сигналізації

На основі плану розташування приміщень підприємства запропоновано наступне розташування датчиків системи охоронної сигналізації:

1) кімнатах директора, бухгалтера, відділів постачання та збуту запропоновано встановити датчик рух. Це дозволить контролювати приміщення на можливість проникнення зловмисника до цих кімнат;

2) на вікна туалету, холу, кімнати охоронника та вхідної двері запропоновано встановити магнітоконтактні (герконові) датчики.

3) в кімнаті охоронника буде розміщуватися пульт системи охоронної системи сигналізації підприємства. За допомогою такого пульта буде відбуватися контроль роботою системи сигналізації;

4) в якості пристрою управління запропоновано використати мікроконтролер, що дозволить виконати програмування з урахуванням

поставлених задач для проектування системи охоронної сигналізації.

Для системи охоронної сигналізації запропоновано використати модулі датчиків нахилу і вібрації SW-18010P – ВД. Даний датчик спрацьовує при розбитті скла вікна або від струсу. На дверях встановлюються геркони СМК-1Э – Г1 для контролю кожного кабінету від НСД у період, коли офіс не працює.

В якості датчики руху запропоновано встановити ІЧ датчик руху HC-SR501 – ІЧ. Це дозволить контролювати переміщення НСД людей за допомогою датчиків руху та інфрачервоного випромінювання.

Датчик руху HC-SR501 - це популярний інфрачервоний (PIR) датчик, який використовується для виявлення руху людини. Ось його технічні характеристики:

1) напруга живлення: від 4.5V до 20V DC

2) споживана потужність: приблизно 50 мкА в режимі очікування, 100 мкА при виявленні руху;

3) частота датчика: в межах 5-10 Гц;

4) кут виявлення: приблизно 120 градусів;

5) дальність виявлення: від 3 до 7 метрів, залежно від налаштувань;

6) час тривалості виводу сигналу: настроюється, зазвичай від 0.3 секунди до 5 хвилин;

7) чутливість: настроюється, зазвичай від 3 метрів до 7 метрів;

8) вихідний сигнал: цифровий (Логічний високий або низький) - може бути підключений до мікроконтролерів або інших пристроїв;

9) виміри: приблизно 32 мм x 24 мм.

Ці характеристики можуть варіюватися в залежності від виробника та версії датчика, тому перед використанням важливо перевірити конкретні технічні характеристики вашої моделі.

Для візуального контролю роботи системи сигналізації використовуються світлодіоди, які розміщуються на передній панелі охоронного пристрою.

Для звукового сповіщення спрацьовування сигналізації застосовується активний динамік 5V (buzzer).

Для керування усіма датчиками застосовується плата мікроконтролера Arduino UNO, яка має 14 цифрових портів.

Таким чином, система охоронної сигналізації має 3 датчика руху і 4 магнітоконтактних датчика.

На рис. 1.14 надано план підприємства з розміщення датчиків та обладнання охоронної сигналізації.

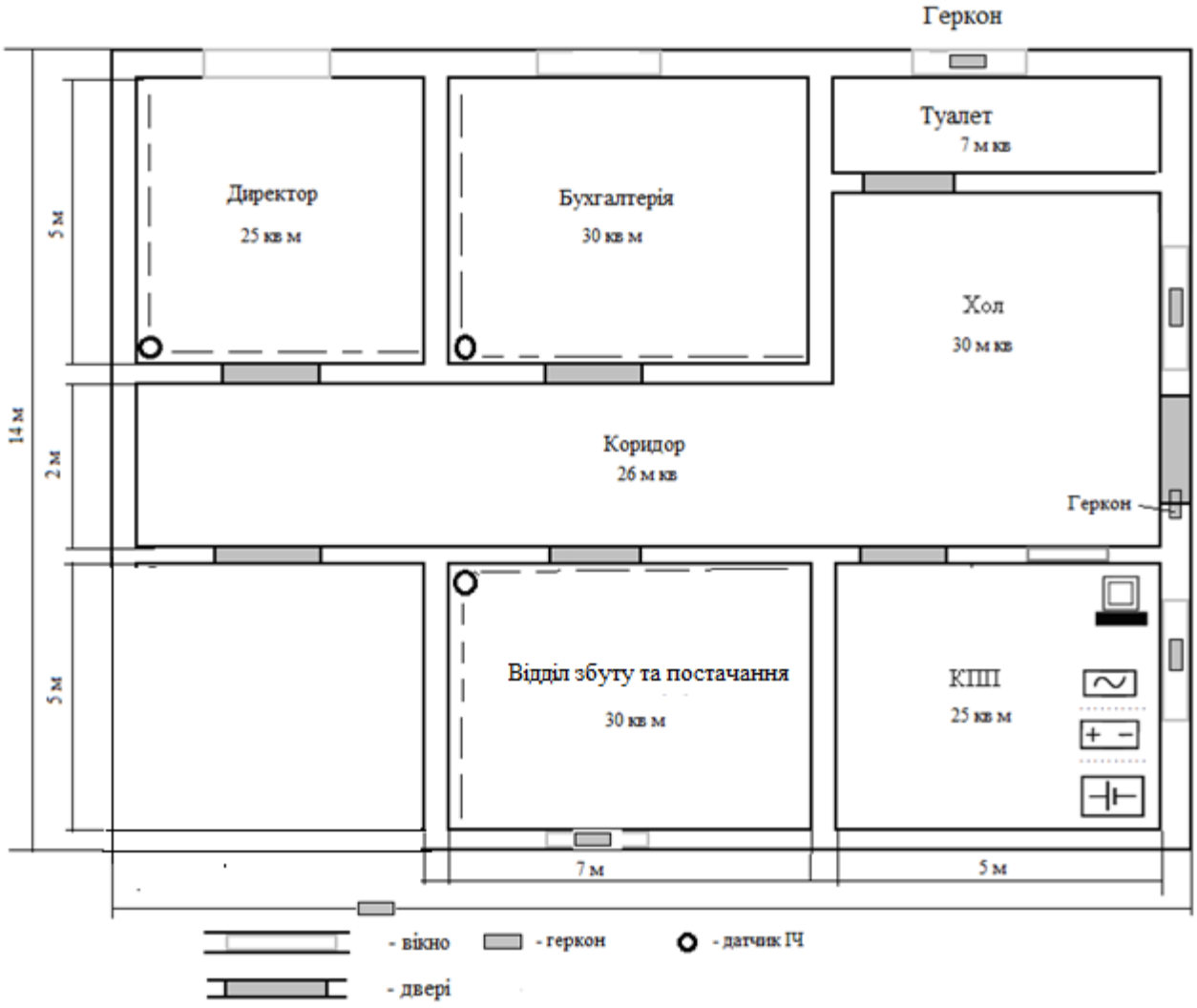


Рисунок 1.14 – План підприємства з розміщення датчиків та обладнання охоронної сигналізації

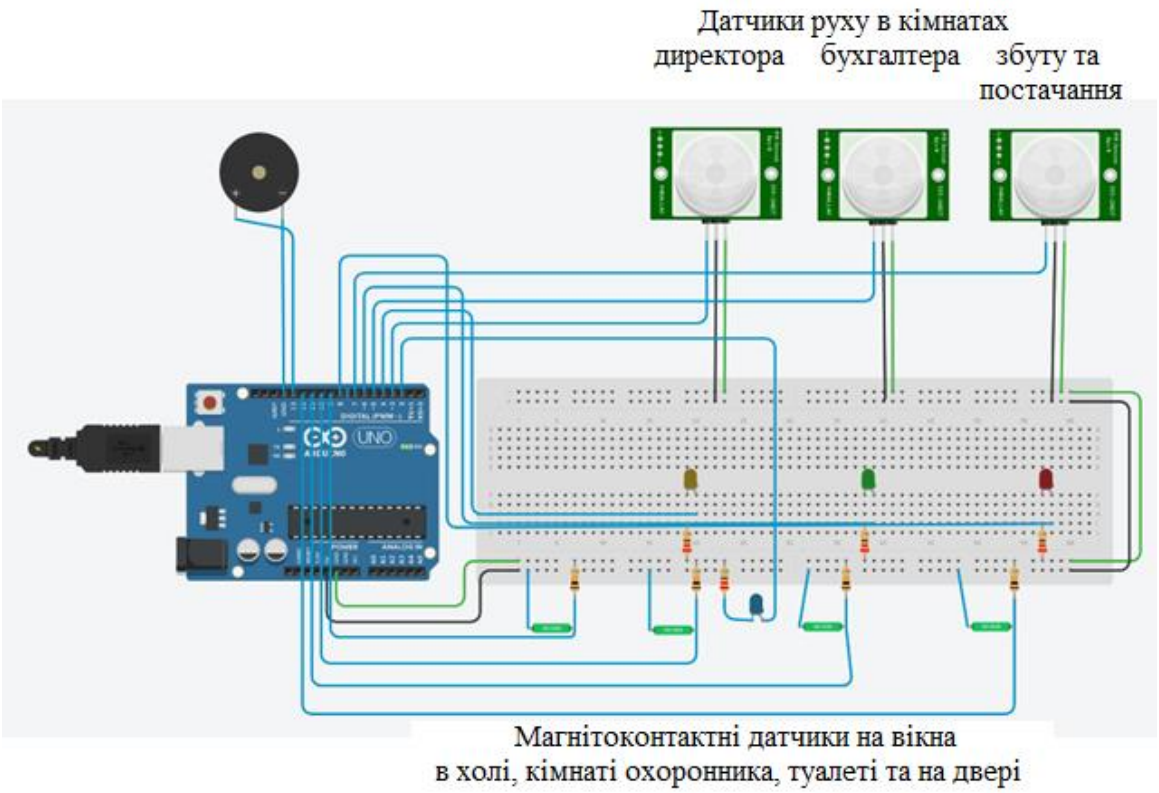


Рисунок 1.15 – Макет електричної схеми системи охоронної сигналізації підприємства

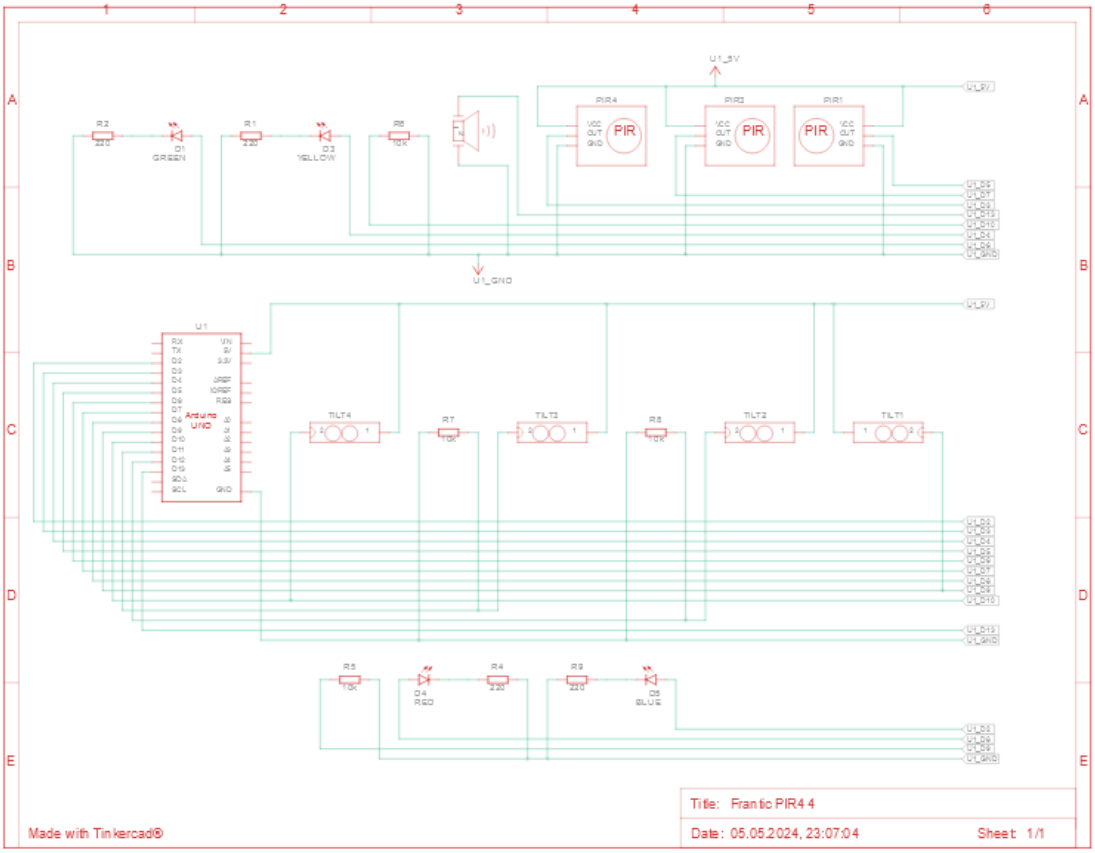


Рисунок 1.16. Схема електрична системи охоронної сигналізації підприємства

Таблиця 3.1 – Перелік радіоелементів схеми електричної системи охоронної сигналізації підприємства

№	Найменування	Кількість	Радіоелементи та компоненти
1	U1	1	Arduino Uno R3
2	PIR1, PIR2, PIR3	3	PIR Sensor
3	PIEZO1	1	Piezo
4	R1, R2, R3, R4	4	220 Ω Resistor
5	D1	1	Green LED
6	D3	1	Yellow LED
7	TILT1, TILT2, TILT3, TILT4	4	Tilt Sensor
8	D4	1	Red LED
9	R5, R6, R7, R8	4	10 kΩ Resistor
10	D5	1	Blue LED

1.3.4 Програмне забезпечення для завантаження мікроконтролера Arduino UNO

Для програмування мікроконтролера Arduino використовується Arduino IDE (Integrated Development Environment) або інші середовища розробки, такі як PlatformIO. Ось кілька опцій:

1) Arduino IDE – це офіційний інструмент для розробки програмного забезпечення для Arduino;

2) PlatformIO – це більш потужний інструмент, який підтримує не тільки Arduino, а й інші платформи. PlatformIO працює як розширення для різних IDE, таких як Visual Studio Code або Atom. Він дозволяє використовувати багато мов програмування та працювати з більшим спектром мікроконтролерів;

3) Arduino Web Editor дає можливість програмувати Arduino без встановлення спеціального ПЗ, ви можете скористатися веб-редактором Arduino;

Для початку роботи з Arduino IDE потрібне наступне:

1) завантажити та встановити Arduino IDE: відвідайте [офіційний сайт Arduino](https://www.arduino.cc/en/software) та завантажте відповідну версію для вашої операційної системи. Після завантаження встановіть програму за інструкціями;

2) вибрати відповідну плату: після запуску Arduino IDE перейдіть в меню "Tools" (Інструменти) -> "Board" (Плата) та виберіть вашу Arduino. Якщо вашої плати там немає, спробуйте "Boards Manager" (Менеджер плат) і встановіть відповідну плату;

3) вибрати порт: знову у меню "Tools" (Інструменти) -> "Port" (Порт) виберіть COM-порт, до якого підключено ваш Arduino;

4) створити новий скетч: вибрати "File" (Файл) -> "New" (Новий) для створення нового скетчу;

5) написати код у вікні редактора. Можна скористатися прикладами, які надає сама Arduino IDE, в меню "File" (Файл) -> "Examples" (Приклади);

6) перевірити код: перед завантаженням коду на вашу плату, скористайтеся функцією "Verify" (Перевірити), щоб переконатися, що код не містить синтаксичних помилок;

7) завантаження коду на плату: після того як код пройшов перевірку, виберіть "Upload" (Завантажити), щоб завантажити його на вашу Arduino;

8) перевірка результату: після завантаження коду перевірте роботу вашого проекту на Arduino.

Це основні кроки для роботи з Arduino IDE. Ви можете докладніше вивчити документацію або відвідати форуми для отримання додаткової допомоги та порад.

В програмі системи охоронної сигналізації використовується команда #define для присвоєння імені портам. Змінні buttonState1 … buttonState4 використовуються для запису початкового нульових станів магнітоконтактних датчиків (герконів). Встановлюється швидкість роботи 9600 бод для монітору послідовного порту за допомогою команди Serial.begin(9600).

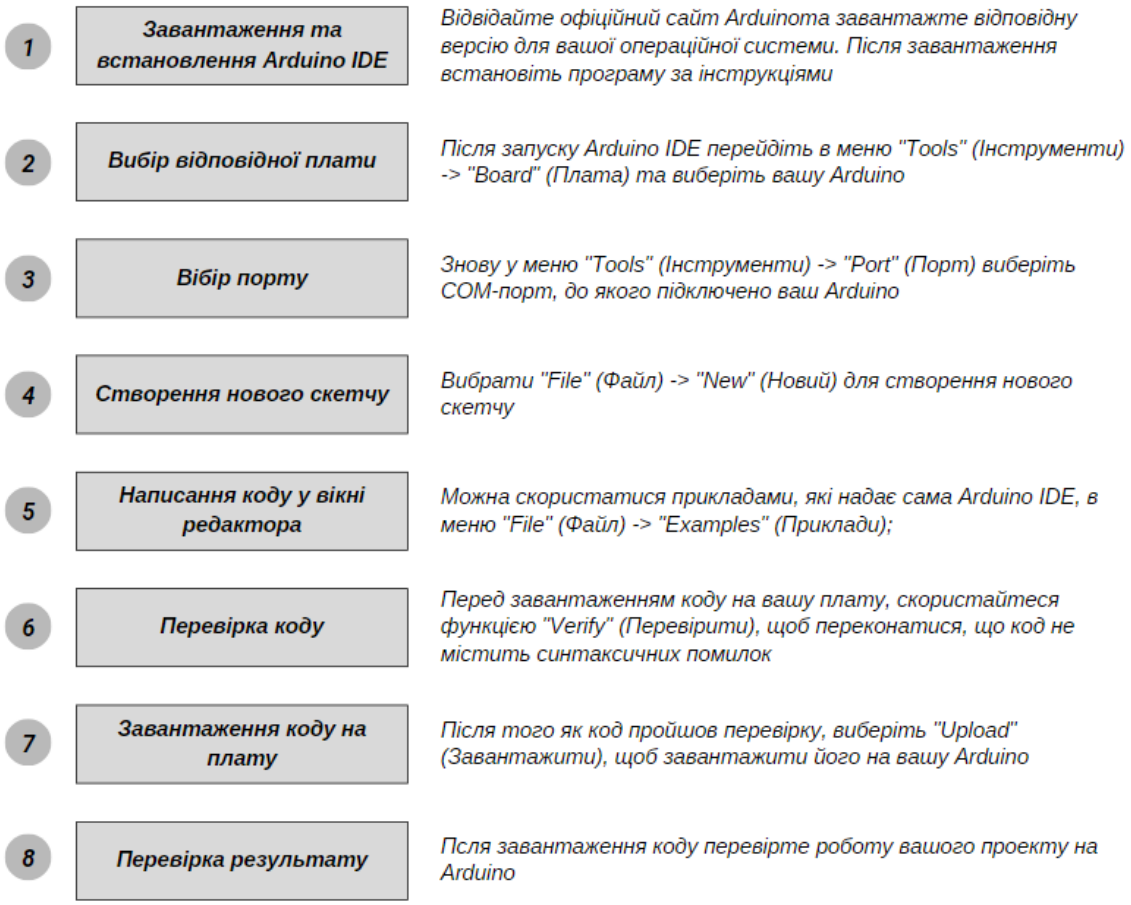


Рисунок 1.17. Алгоритм дій при роботі з Arduino IDE

У частині програмі void setup()у записуються стани датчиків руху в змінні pirVal1 … pirVal3 за допомогою команди digitalRead(PIN_PIRx). Таким же чином записуються стани магнітоконтактних датчиків в змінні buttonState1 … buttonState4. За допомогою команд Serial.println(pirVal1) … Serial.println(pirVal3) відбувається передавання станів у монітор послідовного порту.

За допомогою конструктора if() – else відбувається перевірка кожного стану датчиків. У випадку спрацьовування датчика починає звучати звуковий сигнал певної частоти, що задається за допомогою команди tone(button_Sound, 200, 500), де button_Sound – ім`я порту, 200 – це частота 200 Гц, 500 – це тривалість звуку.

За допомогою digitalWrite(PIN_LEDx, HIGH) встановлюється високий рівень напруги на виході порту PIN_LEDx, що потрібно для свічення світлодіоду з ім’ям PIN_LEDx, коли спрацьовує датчик.

```
#define PIN_PIR1 3 // датчик ІЧВ – кімната директора
#define PIN_LED1 4 // світлодіод - директора
#define PIN_PIR2 5 // датчик ІЧВ - кімната бухгалтера
#define PIN_LED2 6 // світлодіод - відділ бухгалтера
#define PIN_PIR3 7 // датчик ІЧВ - кімната відділу збуту та постачання
#define PIN_LED3 8 // світлодіод - відділ збуту та постачання
#define PIN_button1 9 // геркон - вікно туалету
#define PIN_button2 10 // геркон - вікно холу
#define PIN_button3 11 // геркон - двері
#define PIN_button4 12 // геркон - вікно охоронника

#define button_LED5 2 // світлодіод - хол туалет двері охор
#define button_Sound 13    // звуковий сигнал
int buttonState1 = 0; // геркон - вікно туалету
int buttonState2 = 0; // геркон - вікно холу
int buttonState3 = 0; // геркон - двері
int buttonState4 = 0; // геркон - вікно охоронника



void setup()
 {
  Serial.begin(9600);

  pinMode(PIN_PIR1, INPUT);
  pinMode(PIN_LED1, OUTPUT);
  pinMode(PIN_PIR2, INPUT);
```

```
  pinMode(PIN_LED2, OUTPUT);
  pinMode(PIN_PIR3, INPUT);
  pinMode(PIN_LED3, OUTPUT);
  pinMode(PIN_button1, INPUT);
  pinMode(PIN_button2, INPUT);
  pinMode(PIN_button3, INPUT);
  pinMode(PIN_button4, INPUT);

  pinMode(button_LED5, OUTPUT);
  pinMode(button_Sound, OUTPUT);
}

void loop()
{
  int pirVal1 = digitalRead(PIN_PIR1);
  int pirVal2 = digitalRead(PIN_PIR2);
  int pirVal3 = digitalRead(PIN_PIR3);

  buttonState1 = digitalRead(PIN_button1);
  buttonState2 = digitalRead(PIN_button2);
  buttonState3 = digitalRead(PIN_button3);
  buttonState4 = digitalRead(PIN_button4);

  Serial.println(pirVal1);
  Serial.println(pirVal2);
  Serial.println(pirVal3);



  //Коли виявлено рух
```

```
if (pirVal1)
{
  digitalWrite(PIN_LED1, HIGH);
  tone(button_Sound, 200, 500);

  Serial.println("Director's room");
  delay(1000);
}
else
{
  //Serial.print("No motion");
  digitalWrite(PIN_LED1, LOW);

}

//Коли виявлено рух
if (pirVal2)
{
  digitalWrite(PIN_LED2, HIGH);
  tone(button_Sound, 600, 500);

  Serial.println("Accountant's room");
  delay(1000);
}
else
{
  //Serial.print("No motion");
  digitalWrite(PIN_LED2, LOW);

}
```

```
  // Коли виявлено рух
  if (pirVal3)
  {
    digitalWrite(PIN_LED3, HIGH);
    tone(button_Sound, 1200, 500);

    Serial.println("The room has been completed");
    delay(500);
  }
  else
  {
    //Serial.print("No motion");
    digitalWrite(PIN_LED3, LOW);

  }
// магнітоконтактні датчики
  if (buttonState1 == HIGH)
  {
    // turn LED on
    digitalWrite(button_LED5, HIGH);
    tone(button_Sound,300,100);
  }
  else
  {
    // turn LED off
    digitalWrite(button_LED5, LOW);
  }
  delay(10); // Delay a little bit to improve simulation performance
 if (buttonState2 == HIGH)
  {
```

```
  // turn LED on
  digitalWrite(button_LED5, HIGH);
  tone(button_Sound,500,100);
}
else
{
  // turn LED off
  digitalWrite(button_LED5, LOW);

}
delay(10); //
if (buttonState3 == HIGH)
{
  // turn LED on
  digitalWrite(button_LED5, HIGH);
  tone(button_Sound,700,300);
}
else
{
  // turn LED off
  digitalWrite(button_LED5, LOW);

}
delay(10); //
if (buttonState4 == HIGH)
{
  // turn LED on
  digitalWrite(button_LED5, HIGH);
  tone(button_Sound,900,300);
}
```

```
  else
  {
    // turn LED off
    digitalWrite(button_LED5, LOW);
  }
  delay(10);
   }
```

1.3.5 Перевірка роботи програмного забезпечення та електричної схеми

Tinkercad, оснований на веб-платформі, пропонує симулятор Arduino, що дозволяє вам розробляти, тестувати і навіть взаємодіяти з вашими проектами Arduino без необхідності використання фізичного обладнання. Ось деякі ключові функції цього симулятора:

1) інтерфейс з високим рівнем зручності: інтерфейс симулятора Arduino в Tinkercad легкий у використанні, інтуїтивно зрозумілий, що дозволяє користувачам швидко розпочати проектування;

2) бібліотека компонентів: Tinkercad має широкий вибір електронних компонентів, доступних для використання, включаючи світлодіоди, резистори, датчики, мотори та інше.

3) Drag-and-Drop функціонал: можна легко перетягувати елементи з бібліотеки у віртуальну робочу область, що спрощує процес створення схем;

4) симуляція поведінки: після побудови схеми можна запустити симуляцію, щоб перевірити, як ваш проект працюватиме у реальному часі;

5) кодування в реальному часі: можна написати код для вашого Arduino прямо у Tinkercad, використовуючи C++ або вбудований текстовий редактор. Після цього ви можете збудувати та завантажити програму безпосередньо на симулятор Arduino;

6) моніторінг серійного порту: можна перевірити виведення вашої програми на моніторі серійного порту, щоб відстежувати дані, що виводяться або вводяться вашим Arduino;

7) спільний доступ і відкритість для спільноти: можна ділитися своїми проектами з іншими користувачами, а також використовувати проекти, які створені іншими у спільноті.

Рисунок 1.18. Ключові функції симулятора Tinkercad

Tinkercad Arduino Simulator – це потужний інструмент для навчання, розробки та тестування проектів Arduino без необхідності у фізичному обладнанні.

На рис 1.19 надано зовнішній вид симулятора Tinkercad Arduino Simulator.

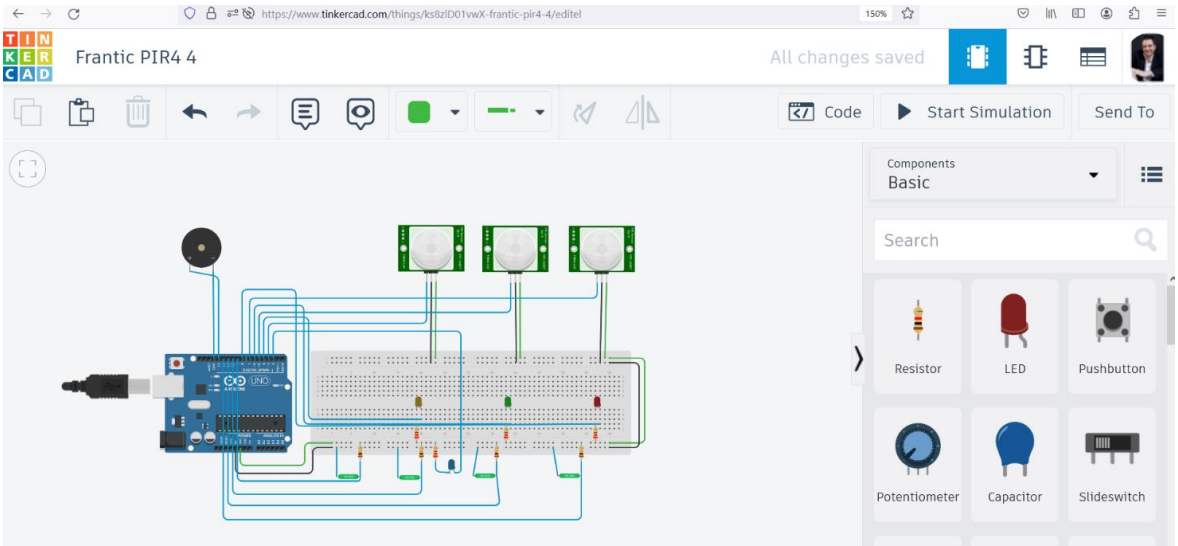


Рисунок 1.19. Зовнішній вид симулятора Tinkercad Arduino Simulator

2. ЕКОНОМІЧНИЙ РОЗДІЛ

2.1 Резюме

Темою даного дипломного проекту є розробка системи охоронної сигналізації підприємства на основі технології Arduino. Ефективність кожного програмного продукту визначається його якістю та ефективністю процесу розробки. Якість ПП визначається наступними складовими: з точки зору користувача; з позиції використання ресурсів; виконання вимог до програмного забезпечення. Проведемо розрахунки визначення трудомісткості розробки даного програмного продукту.

2.2 Розрахунок ціни програмного продукту нормативним методом

2.2.1 Визначення трудомісткості розробки програмного забезпечення

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

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

Таблиця 2.1. Каталог аналогів

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

Для нашого варіанта виділено сірим кольором.

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

Таблиця 2.2. Трудомісткість

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

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера, Кк=0,7÷0,8): Тар = 229 х 0,8 = 183,2 (люд/годин).

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

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

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

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

Для розрахунку необхідні наступні коефіцієнти:

Li – питома вага і-го етапу розробки (див. табл. 2.2.);

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

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

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

Код стадії	Ступінь новизни		
	А	Б	В

ТЗ (L_1)	0,15	0,12	0,12
ТП (L_2)	0,16	0,15	0,11
РП (L_3)	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4. Значення поправочного коефіцієнта, що враховує ступінь новизни

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

Для нашого варіанта виділено сірим кольором.

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

Таблиця 2.5. Значення коефіцієнта ступеня використання в розробці типових програм

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

Для нашого варіанта виділено сірим кольором.

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

Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$Т_{тз}=Та*L_1*К_н=183,2 *0,12*0,7= 15,39 \text{ (люд/годин)} \quad (2.4)$$

Трудомісткість розробки технічного проекту

$$Т_{тп}=Та*L_2*К_н=183.2 *0,11*0,7 = 17,42 \text{ (люд/годин)} \quad (2.5)$$

Трудомісткість розробки робочого проекту

$$Т_{рп}=Та*L_3*К_н*К_т=183,2 *0,61*0,7*0,7=54,76 \text{ (люд/годин)} \quad (2.6)$$

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

Розрахунок зведений у таблицю 2.6

Таблиця 2.6. Розрахунок трудомісткості ПП

Найменування етапів	Розрахунок, годин.		
1	2	3	4
1.ТЗ	$T_{Ртз}$=15,39	$T_{кк}=0,7*N_{тз}$= 0,7*2=1,4	$T_{нк}=0,15*N_{тз}=0,15*2=0,30$
2.Розробка ТП	$T_{Ртп}$=14,12	$T_{кк}=0,7*N_{тп}=0,7*28=19,6$	$T_{нк}=0,15*N_{тп}=0,15*28=4,2$
3.Розробка РП	$T_{Ррп}$=54,76	$T_{кк}=0,7*N_{рп}=0,7*37=25,9$	$T_{нк}=0,15*N_{рп}=0,15*37=5,55$
4.Розробка ПЗ	$T_{пз}=1,5**N_{пз}$= 1,5*30 =45	$T_{кк}=0,7*N_{тз}=0,7*30=21$	$T_{нк}=0,15*N_{пз}=0,15*30$ =4,5
Усього, в т.ч.:	231,56		
- на розробку	$\Sigma T_р$=149,11		
- контроль керівника		$\Sigma T_{кк}$=67,8	
- нормоконтроль			$\Sigma T_{нк}$=14,55

2.2.2 Розрахунок ціни програмного продукту

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

Таблиця 2.7. Розрахунок основної заробітної плати виконавців

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

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

Таблиця 2.8. Розрахунок матеріальних витрат на розробку ПЗ

Найменування матеріальних витрат	Тип, модель	Кількість	Ціна одиниці, грн.	Вартість, грн.
Папір	Лист А4	100	1.5	150,0
Папір	Лист А1	4	15,0	60,0
Разом	-	-	-	$В_{м\,і}$ =210,0
Транспортно – заготівельні Витрати (10%)				$Втр\_з = 0{,}1 \times Вм1$= 0,1х210=21,0
Усього				$В_м = В_{мі} + В_{тр\ з=}$ 231.0

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

Таблиця 2.9. Розрахунок статей витрат планової собівартості

Стаття витрат	Значення, грн.	Формула розрахунку
1. Матеріали	231.0	$В_м$ (див. табл. 2.7)
2. Основна заробітна плата	8521,90	$З_о$ (див. табл. 2.6)
3.Додаткова заробітна плата	852,19	$Зд = 0{,}1 \times Зо$ =8521,90х0,1
4.Відрахування до єдиного фонду соціального внеску	2062,30	$Вє.с.в. = 0{,}22 \times (Зо + Зд)$ =0,22х (8521,90+852,19)
5. Накладні витрати	3408,76	$Внак. = 0{,}4 \times Зо$ =0,4 х 8521,90
6. Повна собівартість	15076,15	$С_{пов}$= $В_м$ +$З_о$ + $З_д$ +Вє.с.в. + Внак.= 231.0+8521,90+852,19+2062,30+ 3408,76

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

$$П=(С_п*Р)/100 \qquad (2.8)$$

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

П= (15076,15*10)/100 = 1507,61грн.

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

3.1 Вступ

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

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

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

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

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

3.3 Гігієнічні вимоги до виробничого середовища

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

3.3.1 Вимоги до приміщення

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

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

3.3.2 Освітлення

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

3.3.3 Шум

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

3.3.4 Мікроклімат

Порушення відповідності ц параметрів мікроклімату впливають на працездатність працівників, їх реакцій, збільшення кількості помилок. Тому в приміщенні повинні бути установлені оптимальні параметри мікроклімату: температура повітря 22-25 ^{0}С, вологість повітря – 40-60%, швидкість пуху повітря – 0,1-0,2 м/с. Для цього приміщення має бути оснащене системами опалення й кондиціювання, що забезпечують постійне й рівномірне нагрівання, циркуляцію й очищення повітря від пилу й шкідливих речовин.

3.3.5 Електробезпека

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

Для попередження поразок електричним струмом необхідно:

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

Для попередження поразок електричним струмом необхідно:

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

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

3.4 Вимоги до організації робочого місця працівника

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео термінала, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

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

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом $+30^0$ до нормальної лінії погляду працюючого. Клавіатуру слід розташовувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого.

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

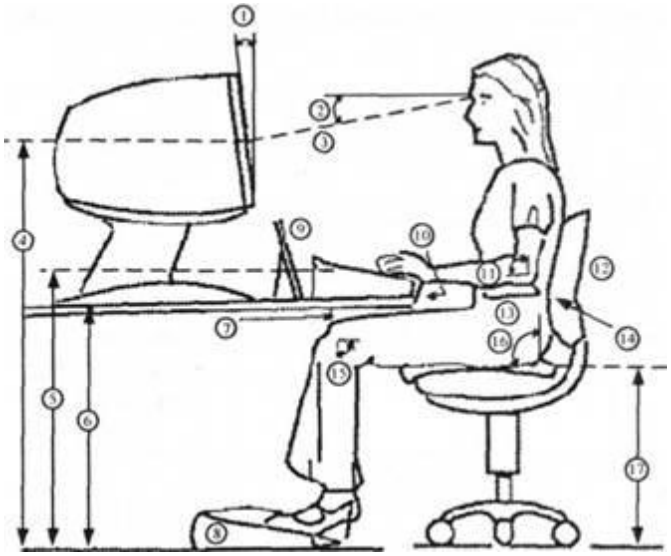


Рис.3.1. Робоче місце і робоча поза користувача комп'ютера

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

3.5 Пожежна безпека

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

Пожежна безпека забезпечується:

-системою запобігання пожежі;

-системою протипожежного захисту;

- організаційно-технічними заходами.

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

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

Рис.3.2. Первинні засоби пожежогасіння

ВИСНОВКИ

При виконанні дипломного проекту розроблена система охоронної сигналізації підприємства на основі трьох датчиків руху та чотирьох магнітоконтактних датчиків. Для завдання розробки було запропоновано використовувати платформу Arduino.

Результати досліджень, виконаних в роботі дозволили встановити, що:

1) платформа Arduino має інтегровану середу для розробки та програмування на мові C++;

2) платформа Arduino має широкий вибір різних мікроконтролерів та датчиків для створення системи охоронної сигналізації;

3) для завдання розробки схеми та програмного забезпечення було використано симулятор Tinkercad Arduino Simulator;

4) застосування симулятору Tinkercad Arduino Simulator дало змогу перевірити правильність написання коду програми та працездатність роботи схеми електричної принципіальної системи охоронної сигналізації.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1 Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Довгий С.О., Воробієнко П.П., Гуляєв К.Д., за загальною редакцією члена-кореспондента НАН України Довгого С.О., Київ “АзимутУкраїна”, 607 стор., 2013 р.

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

3 Шон Харрис. CISSP Посібник для підготовки до іспиту / Шон Харрис // П’ята редакція, 2019. - 875 с.

4 Access control systems. [Електроний ресурс]. – Режим доступу: https://isbc.com/app_area/humans-id/access-control/.

5 Среда разработки Arduino. [Електроний ресурс]. – Режим доступу: http://arduino.ru/Arduino_environment.

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

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

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

ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ

РОЗРОБКА СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ ПІДПРИЄМСТВА НА ОСНОВІ ТЕХНОЛОГІЇ ARDUINO

ДИПЛОМНИЙ ПРОЕКТ

Керівник:
к.ф.н., доцент каф. КБ та ТЗІ ДУІТЗ Стайкуца С.В.
Виконав:
студент групи 4КБ-01 Аршер М.В.

2024

АКТУАЛЬНІСТЬ ТЕМИ

Актуальність роботи *обґрунтована доцільністю створення ефективних і дешевих систем охоронної сигналізації підприємства.*

В дипломному проекті розроблена система охоронної сигналізації підприємства. Для виконання завдання розробки обґрунтовано використання платформи Arduino, яка має всі необхідні датчики і мікроконтролери. Обрано пасивні датчики інфрачервоного випромінювання і магнітоконтактні пристрої на основі герконів. Для управління системою охоронної сигналізації обрана плата мікроконтролер Arduino Uno. Розроблена схема електрична принципіальна системи охоронної сигналізації та відповідне програмне забезпечення. Тестування схеми було проведено в симуляторі Tinkercad.

Мета роботи *– розробка системи охоронної сигналізації підприємства на основі платформи Arduino.*

Об'єкт проектування *– процеси управління датчиками охоронної сигналізації*

Ефективність технічних засобів охорони об'єктів

Технічні засоби безпеки

– це пристрої, програми та системи, призначені для забезпечення безпеки на об'єкті, будівлі або території.

Продуктивність	Мінімальний вплив на продуктивність	Низька кількість помилок
Простота використання	Автоматизація	Висока точність
Моніторинг та звітність	Скалабельність	Оптимізація ресурсів

Компоненти системи охоронної сигналізації підприємства

Різновиди охоронних датчиків

Зовнішній вигляд датчиків руху

Зображення датчика руху

Інфрачервоний датчик руху

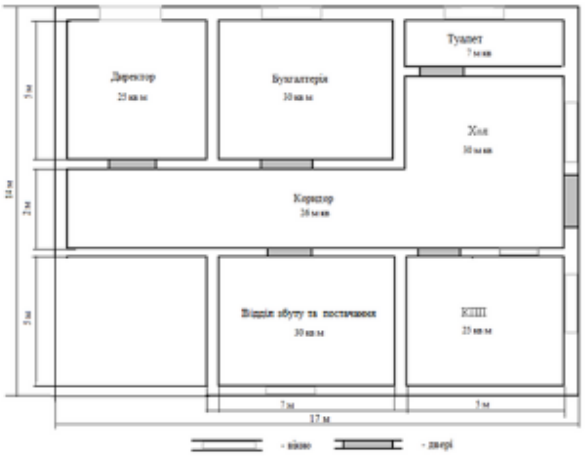
Зовнішній вигляд датчиків руху

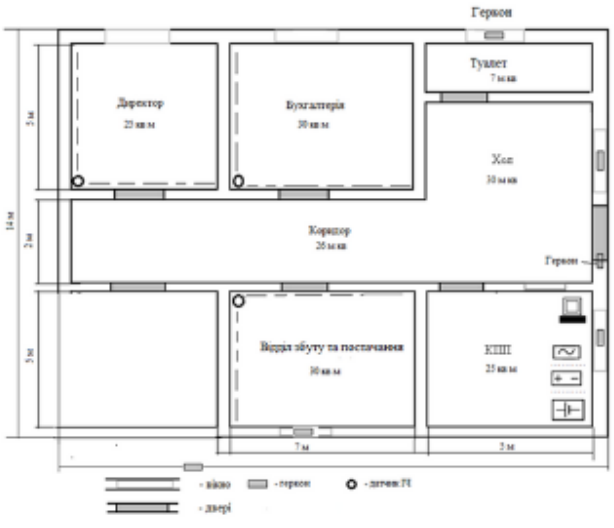
Бездротовий датчик відкриття дверей/вікон Ajax DoorProtect black

Магнітоконтактний датчик Електрон СМК-7ЭП

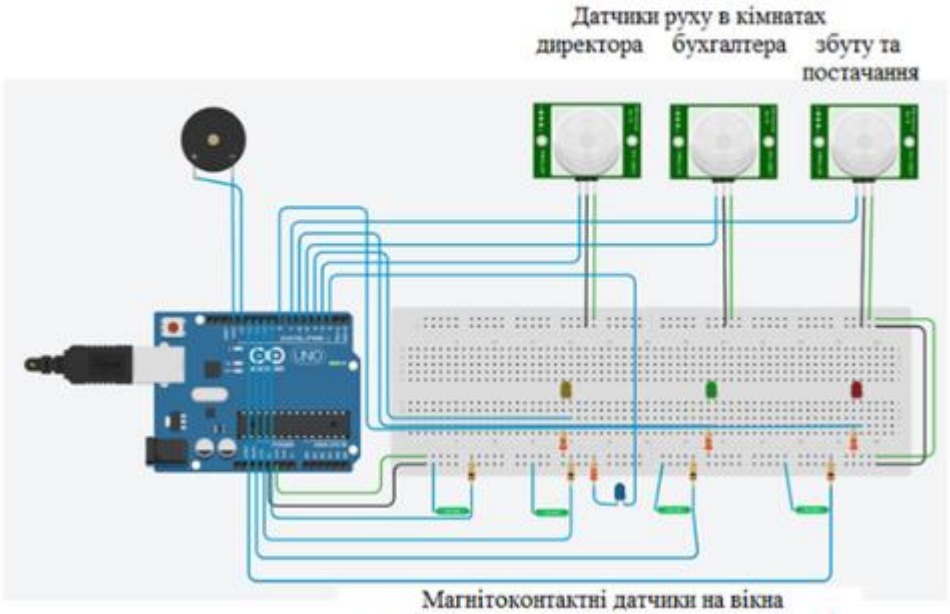
План підприємства для розташування елементів охоронної сигналізації

Розміщення датчиків та обладнання охоронної сигналізації в приміщеннях підприємства





Макет електричної схеми системи охоронної сигналізації підприємства



Алгоритм дій при роботі з Arduino IDE

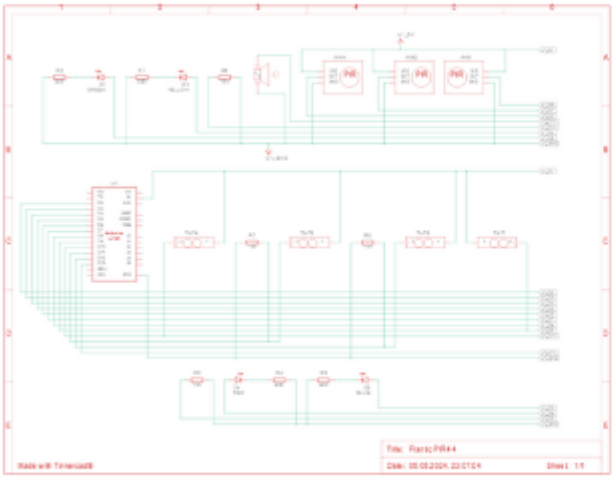
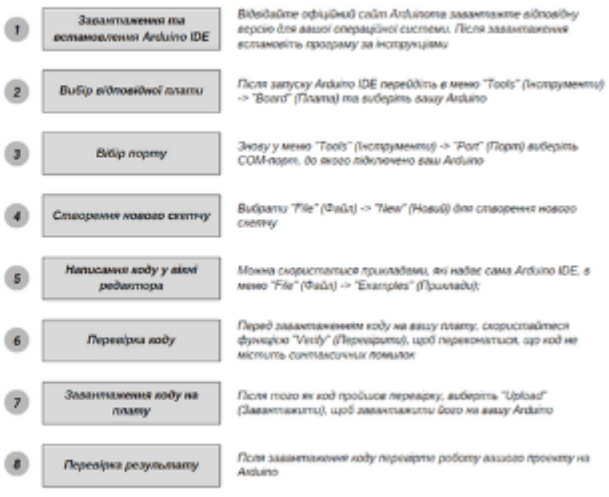


Схема електрична системи охоронної сигналізації підприємства



Алгоритм дій при роботі з Arduino IDE

Деякі параметри датчика руху HC-SR501

Параметри датчика руху HC-SR501:

- *дальність виявлення складає 0 - 7 м;*
- *кут спрацьовування: 110 ° на дистанції до 7 м;*
- *рекомендована напруга живлення складає 4.5 - 12 В;*
- *вихідна напруга логічного рівня: 0 - 3.3 В;*
- *споживаний струм: 65 мА;*
- *робочі температури: -20 - +50 град. Цельсія;*
- *розміри: 32х24 мм*

Плати мікроконтролера ArduinoUNO

Загальні характеристики плати ArduinoUno:

a)мікроконтролер: ATmega328;
b)робоча напруга: 5В;
c)вхідна напруга (рекомендована) - 6-9В;
d)цифрових входів/виходів: 14
(з яких 6 можуть бути використані як ШІМ);
e)аналогових входів – 6;
f)сила струму на входах/виходах: 40 мА;
g)сила струму для 3.3В виходу: 50 мА;
h)пам'ять: 32 кБ з яких 2кб використовується бутлоадер;
i)SRAM: 2 кБ;
j)EEPROM: 1 кБ.
k)частота: 16 МГц
l)USB інтерфейс: CH340

Перевірка роботи програмного забезпечення та електричної схеми

Tinkercad, оснований на веб-платформі, пропонує симулятор Arduino, що дозволяє вам розробляти, тестувати і навіть взаємодіяти з вашими проектами Arduino без необхідності використання фізичного обладнання

Висновки

В проекті проведено розробку системи охоронної сигналізації підприємства на основі трьох датчиків руху та чотирьох магнітоконтактних датчиків. Для завдання розробки було запропоновано використовувати платформу Arduino.

Результати досліджень, виконаних в роботі дозволили встановити, що:

1) платформа Arduino має інтегровану середу для розробки та програмування на мові C++;

2) платформа Arduino має широкий вибір різних мікроконтролерів та датчиків для створення системи охоронної сигналізації;

3) для завдання розробки схеми та програмного забезпечення було використано симулятор Tinkercad Arduino Simulator;

4) застосування симулятору Tinkercad Arduino Simulator дало змогу перевірити правильність написання коду програми та працездатність роботи схеми електричної принципіальної системи охоронної сигналізації.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Аршера Миколи Вікторовича

(прізвище, ім'я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: Розробка системи охоронної сигналізації підприємства на основі технології Arduino

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить 80 сторінки. У пояснювальній записці розглянуто проблеми створення системи охоронної сигналізації для підприємства наведено вимоги та представлено складові засобів охорони. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Аршер М.В. виконував всі етапи розробки проекту, без порушення термінів. Роботу студент виконував в більшій мірі самостійно, з оглядом на рекомендації керівника та отримуючи зворотній зв'язок.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Аршер М.В під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника якісна і він готовий до захисту дипломного проекту.

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Аршер М.В. приймав рішення щодо вибору обладнання, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту

"Державний університет інтелектуальних технологій і зв'язку",
доцент кафедри кібербезпеки та технічного захисту інформації,
помічник декана факультету інформаційних технологій та кібербезпеки

Підпис _____

«10» червня 2024 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Аршер Микола Вікторович

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем та мереж»*

Керівник дипломного проекту (роботи) *Стайкуца Сергій Володимирович*

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) *Розробка системи охоронної сигналізації підприємства на основі технології Arduino.*

Обсяг розрахунково-пояснювальної записки *80* сторінок

Обсяг графічної (презентаційної) частини *14* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту завданню

Представлений на рецензію дипломний проект відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений проблемі створення сигналізації підприємства та складається з пояснювальної записки, додатку з програмним кодом та мультимедійної презентації, що містить приклади роботи програми.

б) характеристика виконання кожного розділу дипломного проекту

Пояснювальна записка складається з основного розділу (аналізу предметної області, проектування моделі, реалізації програмної моделі, тестування програмної моделі), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію та вимоги до техніки безпеки оператора КТ. Економічний розділ проекту містить розрахунок витрат на НДР та реалізацію проекту.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту

Графічна частина складається з 14 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять ілюстративні схеми, скриншоти роботи програмного застосунку, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання графічної частини проекту та пояснювальної записки відмінна, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту *Реалізовано систему охоронної сигналізації підприємства на основні технології Arduino.*

Система охоронної сигналізації може бути впроваджена для невеликого приміщення.

д) основні недоліки дипломного проекту

Для впровадження системи охорони у великі приміщення потрібно передбачити збільшення кількості датчиків.

В деяких частинах пояснювальної записки присутні незначні помилки оформлення.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *Василіу Євген Вікторович*

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

Підпис

«14» *червня* 2024 р.

UNICHECK
by Turnitin

Ім'я користувача:
Катерина Григоріївна Краснокутська

ID перевірки:
1016336608

Дата перевірки:
08.06.2024 23:03:22 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.06.2024 09:12:36 EEST

ID користувача:
100011688

Назва документа: **4КБ-01 Аршер Микола**

Кількість сторінок: **58** Кількість слів: **9587** Кількість символів: **72012** Розмір файлу: **1.29 MB** ID файлу: **1016137389**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

4.29%
Схожість

Найбільша схожість: **2.92%** з Інтернет-джерелом (https://card-file.ontu.edu.ua/server/api/core/bitstreams/4c0773a8-2d0..

4.29% Джерела з Інтернету | **181** ..... Сторінка 60

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи | **5**

Підозріле форматування | **13 сторінок**

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Аршер Микола Вікторович,
здобувач освіти гр. 4КБ-01, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

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

«Розробка системи охоронної сигналізації підприємства на основі технології Arduino»

(автор роботи – Аршер М.В., керівник роботи – Стайкуца С.В.)

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

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

Виконавець _____ / Аршер М.В. /

Керівник _____ / Стайкуца С.В. /

«10» червня 2024 р.