**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Приладобудівний факультет**

**Кафедра автоматизації та систем неруйнівного контролю**

«На правах рукопису»

УДК 681.772

«До захисту допущено»

В.о. завідувача кафедри

_____ Юрій КИРИЧУК
(підпис)

“___”_____2021 р

**Магістерська дисертація**
**на здобуття ступеня магістра**
**за освітньо-професійною програмою «Комп'ютерно – інтегровані технології проектування приладів»**
**зі спеціальності 151 Автоматизація та комп'ютерно - інтегровані технології**

на тему: «Комплексна автоматизована система безпеки на заводі по виготовленню сиру »

Виконав: студент ІІ курсу, групи ПМ-01мп Захаров Єгор Олегович

Науковий керівник к.т.н., доцент Нечай Сергій Олексійович

Консультант

Розробка СТАРТАП-проекту професор, д.е.н. Бояринова Катерина Олександрівна

Рецензент доцент, к.т.н. Добролюбова М.В.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ 2021

# ВІДОМІСТЬ МАГІСТЕРСЬКОЇ ДИСЕРТАЦІЇ

| № з/п | Формат | Позначення | Найменування | Кількість | Примітка |
|---|---|---|---|---|---|
| 1 | А4 | | Завдання на магістерську дисертацію | 2 | |
| 2 | А4 | МД ПМ01МП.05.000 ПЗ | Пояснювальна записка | 100 | |
| 3 | А1 | МД ПМ01МП.05.001 ПН | План розміщення датчиків на території | 1 | |
| 4 | А1 | МД МП01МП.05.002.СХ.01 | Ієрархічна схема системи безпеки | 1 | |
| 5 | А1 | МД ПМ01МП.05.000.СК.02, 03 | Складальні креслення | 2 | |
| 6 | А1 | МД ПМ01МП.05.000.3Д.04 | 3D модель | 1 | |
| 7 | А1 | МД. ПМ01МП.05.000ДТ | Деталювання | 1 | |
| 8 | А1 | МД.ПЛ | Презентаційний лист | 1 | |

| | ПІБ | Підп. | Дата | МД.ВМД | | |
|---|---|---|---|---|---|---|
| Розробн. | Захаров Є.О | | | | | |
| Керівн. | Нечай С.О. | | | Відомість магістерської дисертації | Лист | Листів |
| Конс. | Бояринова К.О. | | | | 1 | 1 |
| Рецензент | доцент, к.т.н. Добролюбова М.В. | | | | КПІ імені Ігоря Сікорського каф. ПБ гр. ПМ – 01мп | |
| Н/контр. | | | | | | |
| Зав.каф. | Киричук Ю.В. | | | | | |

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Приладобудівний факультет**

**Кафедра автоматизації та систем неруйнівного контролю**

Рівень вищої освіти – другий (магістерський)

Спеціальність –151 Автоматизація та комп'ютерно-інтегровані технології

Освітньо-професійна програма Комп'ютерно-інтегровані технології проектування приладів

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Юрій КИРИЧУК

«___»_____20__ р.

**ЗАВДАННЯ**

**на магістерську дисертацію студенту**

Захаров Єгор Олегович

(прізвище, ім'я, по батькові)

1. Тема дисертації «Комплексна автоматизована система безпеки на заводі по виготовленню сиру », науковий керівник дисертації к.т.н. , доцент Нечай Сергій Олексійович, затверджені наказом по університету від « 05 »листопада 2020р. № 3228

2. Строк подання студентом дисертації 13 грудня 2021

3. Перелік завдань, які потрібно розробити: Розробка системи безпеки, розрахунок камери пінхола з габаритами до 10*10*30 см, розробка перемитрального датчику з робочою зоною не менше 80м, примыщення

4. Перелік графічного (ілюстративного) матеріалу 8 аркушів формату А1 які

5. Орієнтовний перелік публікацій стаття в матеріалах конференцій

6. Консультанти розділів дисертації*

_____

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Розробка СТАРТАП-проекту | Професор д.е.н., Бояринова Катерина Олександрівна | | |

7. Дата видачі завдання 30 вересня 2021р.

Календарний план

| № з/п | Назва етапів виконання магістерської дисертації | Строк виконання етапів магістерської дисертації | Примітка |
|---|---|---|---|
| 1 | Одержати у керівника дипломного проекту (МД) затвердженого завідувачем кафедри завдання на МД | 30 вересня 2021р. | |
| 2 | Виконання пояснювальної записки МД | 01 грудня 2021р. | |
| 3 | Виконання розділу розробка СТАРТАП-проекту | 13 грудня 2021р. | |
| 4 | Виконання графічних матеріалів МД | 13 грудня 2021р. | |
| 5 | Подання керівнику для перевірки: ДП та тексту його остаточного варіанту в електронному вигляді, одержання відгука на ДП | 13 грудня 2021р. | |
| 6 | Одержання рецензії на МД | 14 грудня 2021р. | |
| 7 | Захист дипломного проекту в екзаменаційній комісії університету | 20 грудня 2021р. | |

Студент _____ Захаров Егор Олегович

Науковий керівник дисертації _____ Нечай Сергій Олексійович

**Пояснювальна записка**

**до Магістерської дисертації**

**на тему: «Комплексна автоматизована система безпеки на заводі по виготовленню сиру»**

Київ – 2021

## Анотація

В даному документі представлено магістерську дисертацію на тему: Комплексна автоматизована система безпеки на заводі по виготовленню сиру’’складається з 3 розділів, висновку, списку літератури та додатків. Пояснювальна записка містить 98 сторінок, 31 рисунка, список літератури з найменуваннями та додатки.

Тема звіту є актуальною через те, що системи безпеки не втрачають актуальність, на кожному підприємстві чи іншому об`єкті що потребує охорони. Системи встановлюють через їх зручність, інформативність та простоту використання у порівнянні з класичним виконанням, що дозволяє проводити моніторинг за менший час, відслідковувати появу чинників загроз, зробити сповіщення працівників на території зони охорони, а також через велике поле для модернізації та покращення характеристик у порівнянні з існуючими системами.

В сучасних системах є багато недоліків основними з яких є слабкість до втручання; мала зона сповіщення про виникнення небезпек; недостатній час реакції, мала точність. Через це дослідження принципів роботи, побудови систем та знаходження оптимальних конструктрських рішень є актуальним.

## Summary

This document presents a master's thesis on:

The Comprehensive Automated Security System at the Cheese Factory consists of 3 sections, a conclusion, a list of references and appendices. The explanatory note contains 98 pages, 31 figures, a list of references and appendices.

The topic of the report is relevant because security systems do not lose relevance at every enterprise or other facility that needs protection. The systems are installed because of their convenience, informativeness and ease of use compared to the classic version, which allows you to monitor in less time, monitor the occurrence of threat factors, notify employees in the protected area, as well as a large field for modernization and performance compared to existing systems.

In modern systems there are many shortcomings, the main of which is the weakness to intervene; small hazard notification area; insufficient reaction time, low accuracy. Therefore, the study of the principles of operation, building systems and finding optimal design solutions is relevant.

**Зміст**

## Перелік умовних позначень, символів, скорочень і термінів

**СККД система контролю керування доступом.**

**АРМ Автоматизоване робоче місце**

**АС Автоматизована система**

**БД База даних**

**ІД Ідентифікатор доступу**

**КУД Контроль і управлення доступом**

**ПЗ Програмне забезпечення**

**СЗІ Система захисту інформації**

**ВП Виконуючий пристрій**

**ППК Пристрій перегороджуючий керований**

**ПП Перегороджуючий пристрій**

**НС Надзвичайна ситуація**

**ТЗ Технічне завдання**

**ПК Персональний комп'ютер**

## Вступ

Серед основних напрямків научно-технічного розвитку особливу увагу слід приділити засобам захисту промислових зон від втручань. Системи безпеки покликати вирішити питання безпеки які виникають у власників виробництв або офісних будівель. Покращення якості, збільшення напрямків захисту інтегрованих в одну систему безпеки. Знизити затрати на використання та інтеграцію систем. Підвищити точність та об`єктивність моніторингу. Одним з перспективних напрямів є розробки в області сповіщення про виникнення загроз, тривог, несанкціонований доступ до території або деяких зон охорони. Існуючі сповіщувачі покривають в кращому випадку лише зону охорони, але важливо мати можливість сповістити персонал, який знаходиться поза зоною заводу. Вирішити дану проблему можна використовуючи смс-сповіщувачі, але пряма інтеграція в системи безпеки становить велику загрозу для самої системи через недосконалість існуючих протоколів зв`язку. В даній роботі проведена інтеграція в існуючу систему без прямого надання доступу до внутрішньої інформації.

Ще одною з важливих цілей є зменшення вартості пристроїв відеоспостереження та фотофіксації. Це можна досягти за рахунок вилучення об`єктиву та його заміну аналогами.

Запобігання та своєчасна реакція на проникнення на охоронюєму територію також дуже важлива задача покладена на систему безпеки, адже це є першим бар`єром на шляху зловмисника, основними складовими якої є камери спостереження та переметральні датчики.

# 1. Дослідження предметної області

*Система безпеки* - це функціональна система, яка відображає взаємодію інтересів і загроз.

*Система забезпечення безпеки* - сукупність, що представляє єдину цілісність, організаційних, інформаційних, технічних, адміністративних та інших заходів, спрямованих на своєчасне виявлення загроз інтересам підприємства; на припинення та попередження впливів загроз.[1]

До складу системи безпеки підприємства входять:

- Система контролю-доступу
- Система сигналізації
- Система відеоспостереження
- Протипожежна система.

## 1.1.Система контролю доступу

Система контролю доступу відповідає за керування доступом та являє собою сукупність програмно-технічних засобів і організаційних заходів, за допомогою яких вирішується завдання контролю і управління доступом як на сам об'єкт, так і в окремі його приміщення, а також оперативний контроль за персоналом і часом його перебування на території об'єкта. Головним напрямком розвитку систем контролю доступу (СККД) є їх інтелектуалізація, тобто передача максимально можливої кількості функцій зі збору, обробці інформації та прийняття рішень апаратних засобів СККД і комп'ютерів.[1]

Система управління доступом сьогодні - це програмно-апаратний комплекс, який може мати в своєму складі наступні компоненти:

- контролери СККД
- керовані замки
- зчитувачі
- Турнікети та шлагбауми
- шлюзові кабіни Металодетектори
- Комп'ютери та програмне забезпечення

Охоронна сигналізація (ОС) - це електронний пристрій, який дозволить завждибути впевненим у безпеці виробничого приміщення і т.д. Охоронна система розрахована на попередження несанкціонованого доступу в приміщення / будівлі.[9]

Вона складається з охоронної панелі (централі) - приладу, який збирає і аналізує інформацію, що надійшла від охоронних датчиків. Ця ж централь виконує заздалегідь запрограмовані в ній функції, виконувані при спрацювання детекторів. Пристрій також включає в себе панель керування, яка відображає стан тривоги, виконує її програмування, створює повідомлення та відповідає за постановку на охорну та вимкнення охорони об`єкту. До мінімального набору обладнання необхідно включити джерело безперебійного живлення (ДБЖ), кабельну мережу та охоронні датчики.

Датчики поділяються на види в залежності від чинника реакції. Найпоширеніші з них - об'ємні датчики працюючі на інфрачервоному випроміненні (ІЧ-датчики), геркони – магнітоконтактні датчики (найчастіше встановлюються на двері або вікна для фіксування їх відчинення), акустичні, вібраційні, ультразвукові, променеві, ємнісні, та датчики з направленою діаграмою виявлення.[1]

Об'ємні датчики або датчики руху, це ІЧ-перетворювачі, чутливим елементом яких є ПИР елемент. Цей сенсор уловлює теплове випромінювання, при фіксації переміщення світлової плями з одного сектора до іншого він передає інформацію на систему про те що в зоні охорони відбувся рух. Деякі, найбільш технологічні датчики можуть розрізняти людину і домашніх тварин за допомогою порівняння розмірів теплових плям. Перевагою таких сенсорів є ціна, якість та надійність. Системи безпеки що використовують датчиками такого типу найчастіше використовуються для захисту квартир та житлових будинків. Хоча досить нескладно обійти їх систему захисту, наприклад, вдягнути одежу що не пропускає тепло, накритися ковдрою одяг або закрити вікно датчика. З цього можна зробити висновок що найкращім випадком буде використовувати їх в зв'язці з ними інші типи охоронних датчиків.

Після камер другою лінією охорони є магнітоконтактні (геркони). Ці сповіщувачі встановлюються в дверних рамах та вікнах і відстежують їх відчинення. Два магніти встановлюються паралельно один до одного: один на рухомої частині двері або вікна, а інший на нерухомій його частин, коли контакт між двома магнітами втрачається, геркон спрацьовує та передає сигнал на панель охорони. Цей тип датчиків найдешевший, дуже надійний і з мінімальним споживанням струму. Хоча система охорони яка втілює лише

такі датчики є ряд недоліків, таких як: проникнення на територію охоронюваного приміщення не відчиняючі вікна або двері - зловмисники можуть проникнути, припустимо, через шахти вентиляції або просто розбити скло що дозволить не відчиняти раму, через це геркон не спрацює. Тому використання таких датчиків в ОС рекомендується в комбінації з іншим типом датчиків, наприклад, акустичних датчиках розбиття скла або встановлення на місця можливого проникнення перемитральних датчиків.[1][9]

Акустичні датчики реагують саме на звук певної частоти - в тому числі, звук скла коли воно розбивається. Найсучасніші з них мають мікропроцесор, який аналізує діаграму звуку і не переплутає звук розбитого скла з іншим звуком. Пам'ять таких датчиків має попередньо закладені звуки розбиття різних типів скла, або звуки з якими руйнується цегла або зминається залізо. Це може бути звичайне скло, скло армоване, триплекс. Цей фактор значно знижує можливість випадкового спрацьовування охоронної системи.

Вібраційні датчики можуть працювати як самостійно так і в парі з акустичними, вони напрямлені на захист стін від пролому та передача інформації про те коли відбуваються такі ситуації, сейфів від розтину і вікон від розбиття. З назви можна зрозуміти що вони реагують на вібрацію. Ці датчики досить складні в налаштуванні і допускають більше помилок ніж інші. Вони чутливі до роботи великих механізмів, будівельної техніки, руху трамваїв, поїздів. Але є випадки коли їм немає альтернатив.

Принцип роботи ультразвукових датчиків - локатор. Вони випускають і приймають ультразвукові коливання. Якщо в їх робочу зону потрапляє рухомий предмет, змінюється довжина хвилі відповідно до закону Доплера. Це слугує приводом до спрацювання сигналу датчика. Ці датчики є незамінними в цехах з високою температурою та коридорах з великою довжиною.

Наступним розглянутим видом є променеві (в деякій літературі позначаються як периметральні), вони слугують для того щоб мати можливість перекрити значні простори, дані перетворювачі складаються з приймача і передавача. При перетині променя який неможливо побачити оком без додаткової апаратури він спрацьовує. Цей тип перетворювачів коштує значних коштів та дуже примхливі до місця встановлення та налаштування, їх в основному використовують для забезпечення безпеки периметра. Переметральні сенсори встановлюються вздовж паркану та працюють постійно не зважаючи на умови зовнішнього середовища.[1][9]

Для охорони особливо важливих предметів використовують ємнісні датчики. Сейфі, предмети мистецтва не можуть обійтись без допомоги саме цього типу. Принцип роботи заснований на створенні поблизу об'єкту, що охороняється поля з певною ємністю. При попаданні всередину будь-якого предмета ємність поля міняється, що в свою чергу призводить до спрацьовування охоронної сигналізації. Цей тип датчиків дуже складний в налаштуванні, досить дорогий та потребує значної площі для розміщення.

Ще одним типом є спецефічні інфро-червоні датчики з направленою діаграмою виявлення, його будову доповнює спеціальна лінза. У напрямку і формі діаграми спрямованості існує три типи таких датчиків: штора, що працює в вертикальній або горизонтальній площині, завіса (напівсфера), коридор, що по суті є вузьким промінем. Назва цих датчиків відповідає за напрямок їх використання.

Охоронна сигналізація забезпечує наступні заходи безпеки:

- Створення фізичних перешкод на шляху порушника
- Виявлення зловмисника на ранній стадії
- Поетапна оцінка ситуації
- Заходи купування дій вторгнення
- відеодокументування
- спрацьовування тривоги
- Багато іншого

Сучасні системи безпеки зможуть своєчасно інформувати вас про проникнення сторонніх осіб на територію, що знаходиться під охороною.

## 1.2.Системи протипожежного захисту

Системи протипожежного захисту - це комплекс технічних засобів, встановлений за об'єкті, який призначений для виявлення, локалізації та ліквідації пожежі без втручання людини, захисту людей, матеріальних цінностей та довкілля від впливу небезпечних факторів пожежі.Системи протипожежного захисту в усьому світі і в Україні зокрема строго регламентуються. Вимоги до них описані нормативними документами (ДБН, ДСТУ та ін.) А також Законами України. З кожним роком норми щодо пожежної безпеки об'єктів все більше посилюються, приводяться у відповідність європейським EN.[2][3]

Вся діяльність в цій галузі стандартизована і сертифікована - виробництво, проектування, впровадження та обслуговування.

- До складу систем протипожежного захисту входять
- Система пожежної сигналізації
- Автоматична / автономна система пожежогасіння
- Система оповіщення про пожежу та управління евакуацією
- Система протидимного захисту
- Система централізованого пожежного спостереження
- Система диспетчеризації СПЗ

### 1.3. Схема системи безпеки

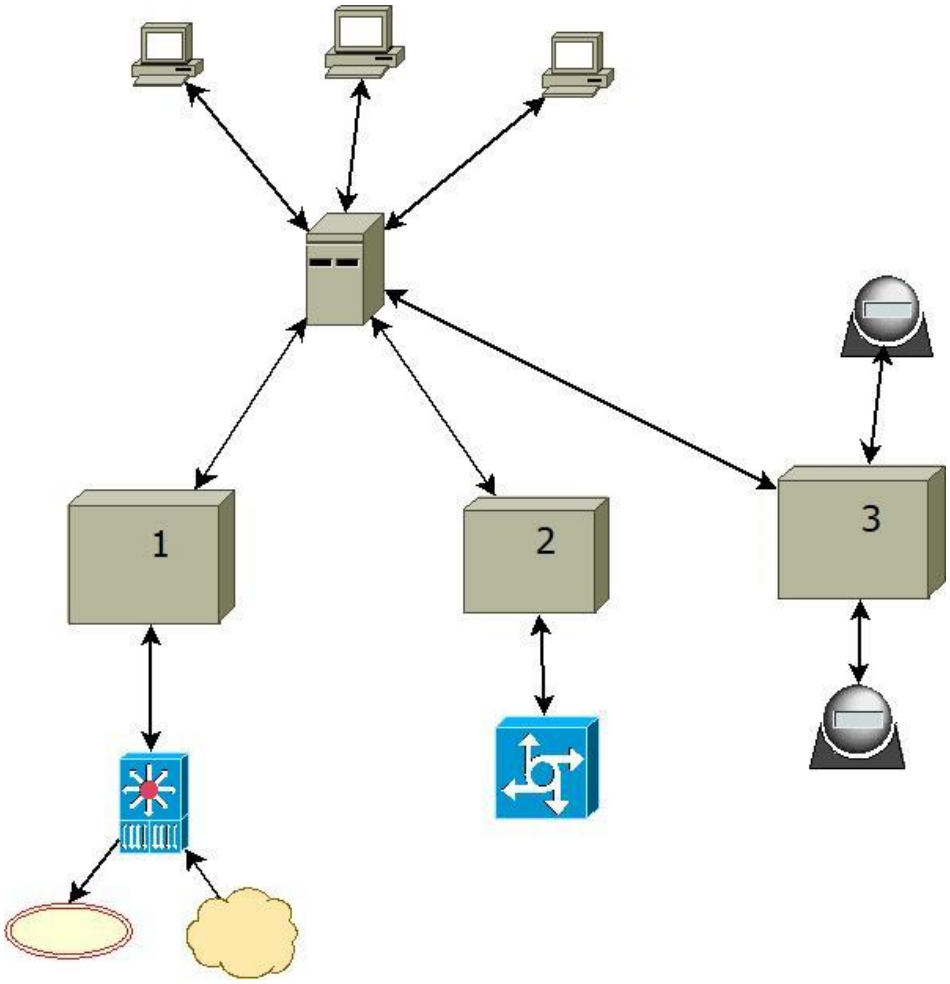


Рисунок 1.1. Логічна схема системи безпеки

На рисунку 1.1 зображено приклад системи безпеки. Серцем цієї системи є сервер на якому встановлено відповідне ПО. Прикладом такого по

є Building Integration System від компанії Bosch. Будь-яка система безпеки повинна контролюватися людиною. Для керування та контролю за системою розміщують місця операторів. Такі місця розміщують на КПП та в централізованій кімнаті охорони. Задачею операторів є своєчасна реакція на будь-які надзвичайні ситуації до яких можна віднести проникнення постороньої особи на об'єкт охорони, пожежу, розбите скло та ін.[9]

Ця інформація потрапляє на сервер з контролерів(1, 2, 3). Кожен контролер може відповідати не лише за певний напрямок, але для загальної схеми таке зображення є оптимальним.[1]

На даній схемі контролер 1 відповідає за отримання інформації з протипожежних датчиків, таких як: димові, газові, теплові, датчики полум'я. Інформація з контролера передається на сервер де в автоматичному режимі приймається рішення щодо ситуації. Одним з таких рішень може бути ввімкнути розприскувач води, або припинити доступ кисню до кімнати, перекривши вентиляційну кришку, що дасть змогу локалізувати пожежу.

Контролер 2 відповідає за систему контролю-доступу. До її функцій входить контроль за переміщенням людей на території об'єкту та своєчасна реакція на несанкціоноване знаходження людини чи рухомої техніки на об'єкті охорони. Таким чином датчик відкриття дверей фіксує їх відкриття і передає цю інформацію на сервер, який порівнює цю інформацію з системою контролю в яку не поступало інформації о намірі санкціонованого відчинення, такою інформацією може бути прикладання картки до зчитувача, або біометрична ідентифікація, таким чином програмне забезпечення розуміє що виникло несанкціонований доступ та подає сигнал тривоги, викликає службу охорони, блокує вікна (наприклад додатковими захисними шторами).

Під цифрою 3 знаходиться блок обробки відео. На який потрапляє відео з камер спостереження. Цей блок відповідає за шифрування відеопотоку з камер спостереження та передачу її на сервер. Який в свою чергу передає його операторським місцям.[10]

### 1.4.Складові частини системи контролю доступу

Систему контролю доступу можна поділити на три складові:

Збір даних.

Складова реакції.

Керуюча частина.

За збір даних відповідають датчики. Такими датчиками є

Датчик розбиття скла

Датчик відчинення дверей

Зчитувач карт

Реакція виконується застосуванням засобів таких як дистанційні замки, штори, сирени.

Керуючою частиною виступає контролер який виносить вирок щодо дій.

### 1.5. Датчики виявлення розбиття скла

Сучасні датчики виявлення розбиття скла (ДРС) бувають двох видів:

- акустичні;
- ударно-контактні.

Як і інші технічні засоби сигналізації, датчики розбиття скла можуть бути адресними і безадресними. У свою чергу адресні бувають як провідними, так і бездротовими. Підключення цих технічних засобів здійснюється залежно від виконання. При живленні шлейфом сигналізації датчики підключаються паралельно з дотриманням полярності (рис.1.2). При спрацьовуванні вони збільшують струм споживання, що відстежується приймально контрольним приладом.

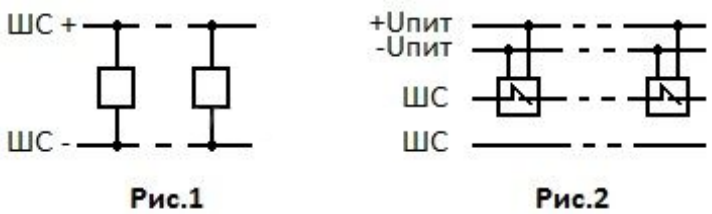


Рис.1 Рис.2

Рисунок 1.2 Підключеня датчики розбиття скла

Такий спосіб підключення трапляється досить рідко. Він характерний для ударно-контактних сповіщувачів типу "Вікно" про які інсталятори починають поступово забувати.

Датчики з окремим живленням (таких більшість) мають контакти реле, які у черговому режимі замкнуті, а при виявленні розбиття скла розмикаються.

Схема їх підключення наведено малюнку 2. Полярність шлейфу не принципова.

Адреса підключаються як на малюнку 1, тільки при спрацьовуванні передають на контрольну панель відповідний код. Бездротові, звичайно, не підключаються - їх адреса прошивається в приймачі і вся інформація передається в кодовому вигляді по радіоканалу.[5]

### 1.6. Акустичні датчики розбиття скла

Це найпоширеніші на даний момент сповіщувачі.

Принцип їхньої дії полягає в аналізі спектра звукових частот, що виникають при розбиванні скла. Мікропроцесорна обробка сигналу покликана мінімізувати хибні спрацьовування та підвищити достовірність виявлення.[1][9]

Популярність акустичних датчиків зумовлюється тим, що виявлення відбувається безконтактно. Це зручно, оскільки такий підхід не вимагає приклеювання сповіщувача до заскленої поверхні.

Сповіщувач виконаний у вигляді одного блоку і складається з друкованої плати 1, кришки 3 основи 3 і мікрофона 4, вбудованого в двопозиційний тримач 5 (додаток А, рисунок А.1). На підставі знаходяться отвори, що розкриваються, для введення проводів 6 і кріплення сповіщувача на стіні і стелі 7, а також в кутку 8. На платі є 5 пар контактів для зміни режимів роботи за допомогою установки перемичок (додаток А, малюнокА.2). Під кришкою розташовані клеми під'єднання проводів живлення "+"і "-", шлейфу сигналізації "ШС", та виносного елемента "R", а також контакти 13 для встановлення перемички "Т", 10 - для перемички "П", 9 - для перемички "І", 11 – для перемички "Ч", 12 – для перемички "Р". Перемички служать для

керування режимами роботи сповіщувача. Конструкція сповіщувача зображена на рис. 1.3.

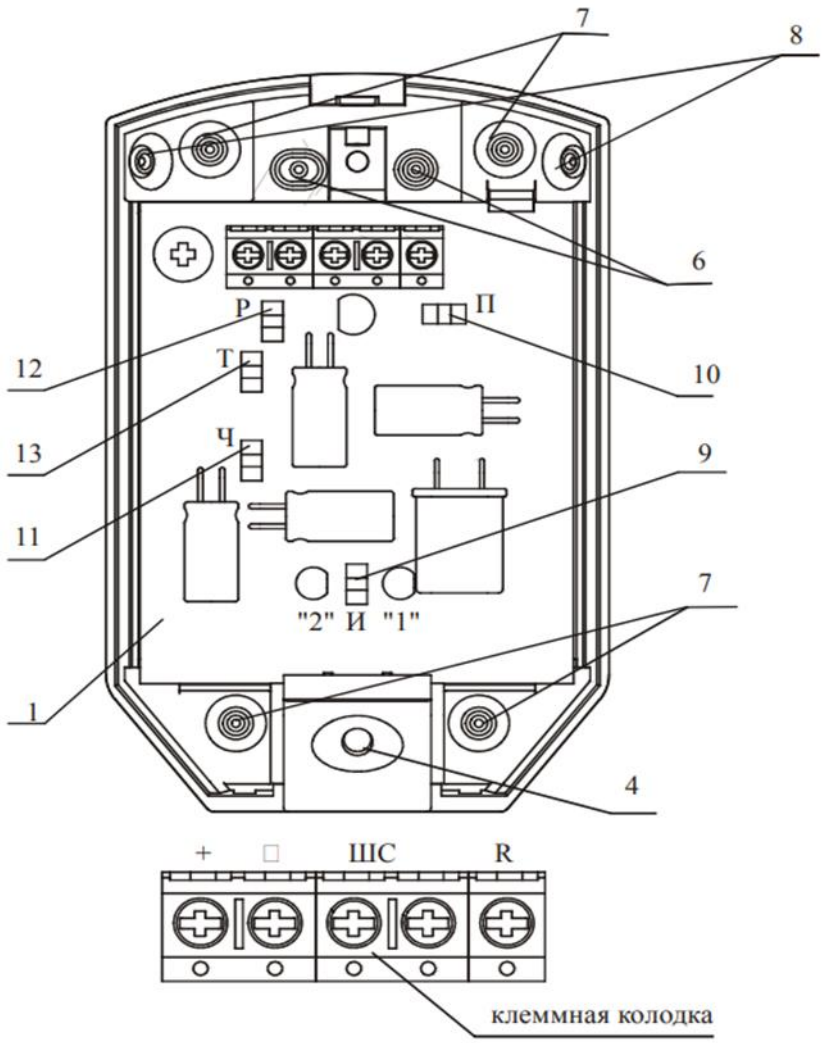


Рисунок 1.3 Конструкція акустичного сповіщувача розбиття скла.

## 1.7. Ударно-контактні сповіщувачі

Існує два типи:

Вікно;

ДІМК.

Вікно є комплектом датчиків розбиття (ДРС), які наклеюються на контрольоване скління і блоку обробки сигналу (БОС), який відстежує їх стан. Залежно від модифікації до одного БОС підключаються кілька ДРС, які

можуть контролювати скло завтовшки від 2,5 до 8 мм, у тому числі покриті полімерною плівкою.

Підключається цей сповіщувач за схемою, наведеною на рис.1 і отримує живлення шлейфу сигналізації.

Реагує на розбиття скла, а також появи на ньому тріщин, які не спричиняють руйнування. Це може стати в нагоді при виявленні вирізування частини скління.

Наступний сповіщувач – ДІМК (датчик інерційний магнітоконтактний). У його корпусі розміщені геркон та магніт на рухомій пластині.

При відхиленні сповіщувача від вертикальної площини на 20о більше за рахунок відхилення пластини з магнітом відбувається розмикання контактів геркона.

Крім того, датчик спрацьовує при неруйнівному ударі по склу, а також його вилучення з рами або вилучення рами цілком.

## 1.8. Датчик відчинення дверей (Геркон)

Влаштований такий контакт в такий спосіб. До сердечника 3 з магнітом'якого матеріалу закріплені контакти 1 і 2 через ізолюючі прокладки 5. Контакти 1 та 2 виконані з того самого магнітом'якого матеріалу що і серцевина. Коли котушка 4 пропускає струм до осердя 3, через це виникає магнітне поле та контакти 1 і 2 намагнічуються та замикаються. Розмикання контактів відбувається у разі припинення току струму через котушку. Геркон зображено на рис.1.4.[5]

Геркони є по своїй суті контактами і наслідуючи їх вони можуть бути нормально – розімкненими, що перемикають (1 перемикаючий контакт) та ті що працюють на розмикання (2нормально - замкнутий контакт).

За ознаками конструктивно - технологічним геркони діляться на дві великі групи: з сухими та з вологими контактами. Перший різновид так і називається сухими герконами, а другий герконами з вологтм контактом. Власне, у роботі сухих герконів, порівняно із звичайними контактами, нічого особливого немає.

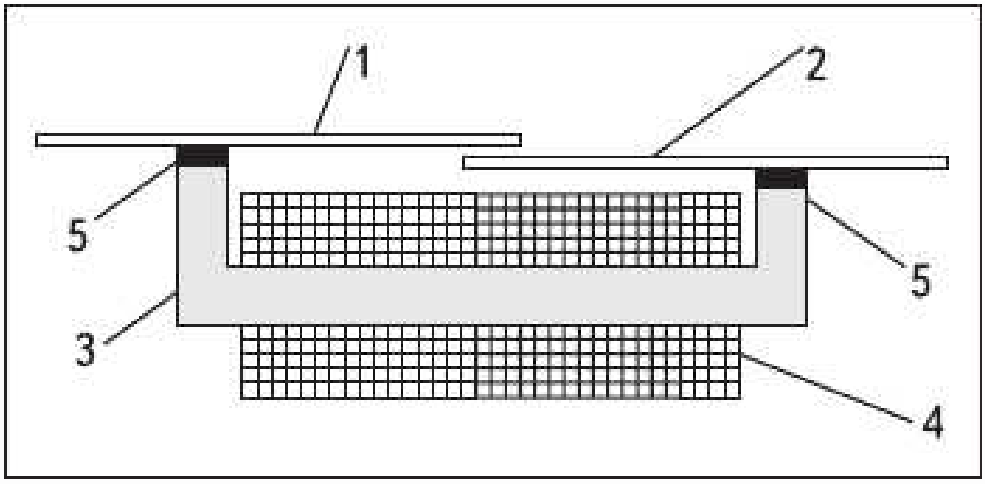


Рисунок 1.4. Геркон.

Різновиди герконів

У ртутних герконах усередині герметичного скляного корпусу, крім контактів, знаходиться ще крапелька ртуті. Призначення цієї ртутної крапельки - змочування контактів під час спрацьовування для поліпшення якості контакту за рахунок зменшення перехідного опору, а також для позбавлення від брязкоту контактів.[5]

Дребізжанням називається вібрація контактів при замиканні і розмиканні, що при одночному спрацьовуванні призводить до багаторазової комутації переданого сигналу, а також до значного збільшення часу спрацьовування.

Конструкція різних типів герконів представлена рисунку 1.5.

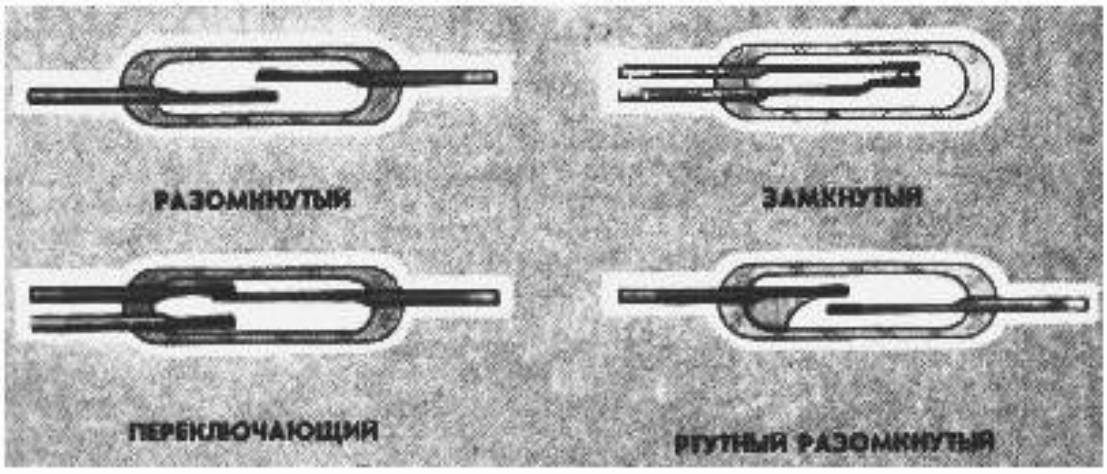


Рисунок 1.5. Конструкція різних типів герконів.

Усі геркони виглядають як скляний балон, всередині якого знаходиться контактна група. Контакти є магнітні сердечники, вварені в торці балона. Зовнішні кінці сердечників призначені для підключення до зовнішнього електричного кола.

Найбільшого поширення набув геркон із контактною групою, що працює на замикання або, як показано на малюнку «розімкнутий». Кожен контакт – сердечник виконаний з феромагнітного пружного дроту, що розплющений до прямокутної форми. Для виготовлення сердечників застосовується пермалоєвий дріт діаметром 0,5 - 1,3 мм залежно від потужності геркона і, відповідно, його габаритів.

Безпосередньо контактуючі поверхні вкриті благородним металом, золотом, паладієм, родієм, сріблом та сплавами на їх основі. Таке покриття не тільки зменшує перехідний опір, а й сприяє підвищенню стійкості корозійної контактної поверхні.

Внутрішній простір балона заповнений інертним газом (воднем, аргоном, азотом або їх сумішшю) або просто вакуумований, також сприяє зменшенню корозії контактів та підвищенню їх надійності. При виготовленні осердя розташовують таким чином, щоб між ними залишався зазор певного розміру.[5]

Принцип роботи геркона.

Для того, щоб викликати спрацювання контактної групи, необхідно довкола геркона створити магнітне що матиме достатню напруну. При цьому абсолютно не важливо, як це поле буде створено або просто постійним магнітом, або електромагнітом. Силові лінії зовнішнього магнітного поля намагнічують внутрішні контакти – осердя геркона, внаслідок чого вони долають сили пружності, притягуються та замикають електричний ланцюг.

У таких випадках контактори будуть знати, що, коли навколо них є достатньо напружене магнітне поле: електромагнітного поля достатньо, щоб досягти, або якщо ви взяли з собою спеціальний постійний магніт, контакти відразу розімкнуться. Знання магнітного поля визначить вихідну точку контактних знань. Однак можливий рух некритичним способом, коли контакт може перемикатися на три функції одночасно, де контакт може виконувати три функції одночасно. Дещо по-іншому діє геркон, що працює на розмикання. Його магнітна система влаштована так, що при впливі магнітного поля, контакти – сердечники намагнічуються одночасноо, тому відштовхуються один від одного, розмикаючи електричний ланцюг.[5]

У геркона, що перемикає, один із трьох контактів, як правило, нормально - замкнутий виконується з металу немагнітного, а обидва нормально - розімкнутого контакту з феромагнітного, як було сказано трохи вище. Тому при дії на геркон магнітного поля нормально розімкнені контакти просто замикаються, а немагнітний нормально - замкнутий, залишаючись на своєму початковому місці, розмикається.

Звичайно, магнітне поле є завжди, наприклад магнітне поле Землі. І не можна, як би, сказати про відсутність магнітного поля зовсім. Але магнітне поле Землі для спрацьовування геркона недостатньо, тому їм можна знехтувати і сказати про відсутність магнітного поля, у цьому випадку зовнішнього.[5]

## 1.9. Зчитувачі карт

Вразливість та захищеність карт доступу СККД

Карта доступу – це ідентифікатор користувача, на якому міститься інформація – ключ, що відкриває двері або доступ до ресурсів. Важко уявити сучасний світ без контактних та безконтактних технологій ідентифікації.

Використання банківських карток (з магнітною смугою, картки з чіпом EMV, безконтактні платежі PayPass, payWave); RFID-карти для транспорту, сфери розваг та програм лояльності: видача полісів ЗМС та соціальних карт москвича, і, звичайно ж, карти фізичного доступу та логічного доступу до комп'ютера та IT-ресурсів компанії – найбільш яскраві приклади повсюдного застосування карт доступу.[6][7][8]

При цьому «карта» – досить умовне поняття, тому що ідентифікатор може бути у формі брелока, тега, мітки тощо. .

Саме тому питання безпеки передачі даних від ідентифікатора до зчитувача як ніколи є актуальним. Ступінь ризику копіювання інформації з карток та їх клонування збільшується щодня, і це змушує більш свідомо підходити до вибору технологій, що забезпечують безпечну ідентифікацію.

Вразливість карт доступу. Як правило, вразливість оцінюють за трьома основними загрозами, виявленими в процесі експлуатації безконтактних

карток: конфіденційність даних, повторне відтворення та клонування карток доступу.

Незахищеність конфіденційних даних

Незахищеність конфіденційних даних, коли ідентифікатор зберігається у відкритому вигляді і ніяк не захищений від зчитування, робить картку доступу та всю систему найбільш уразливою, дозволяючи зловмисникам отримати не лише доступ до об'єкта, а й інформацію про власника картки. Проблема вирішується використанням алгоритмів шифрування DES, 3DES, AES.

Повторне відтворення. Так як при кожному читанні карти передається та сама інформація, її можна перехопити, записати і повторно відтворити для отримання доступу до приміщення. Захистом від повторного відтворення є взаємна автентифікація карти доступу та зчитувача. [6][7][8]

Клонування (копіювання) карт доступу. Найпоширеніший спосіб обходу контролю доступу – клонування карток програматором непомітно для власника картки. Якщо інформація зберігається на карті у відкритому доступі та не захищена від несанкціонованого зчитування (наприклад, у картах стандарту Em-Marine) – картка доступу може бути скопійована.

Зчитування зловмисником даних з карти відбувається за допомогою компактного і доступного за ціною приладу - дублікатора. Для цього необхідно лише наблизитися до карти, послати на неї з дублікатора сигнал, що імітує сигнал зчитувача, отримати сигнал у відповідь з карти, записати його в пам'ять пристрою, а потім на бланк карти. [6][8]

Тим не менш, за допомогою програмного забезпечення можна налаштувати розмежування доступу (диверсифікацію ключа), що забезпечить більшу надійність СККД, що використовують подібні карти. Захищеність карт доступу.

Серед усіх радіочастотних технологій найбільш уразливі з погляду зазначених вище параметрів карти 125 КГц. Однак, карти не всіх стандартів піддаються такому простому злому, багато сучасних ідентифікаторів захищені від подібних загроз за допомогою прогресивних технологій. Наприклад, захист карт доступу 13,56 МГц забезпечується за рахунок взаємної автентифікації між картою та зчитувачем, процес якої відбувається у зашифрованому вигляді з формуванням та підтвердженням ключа диверсифікації. [7][8]

Питання захищеності технологій ідентифікації не менш актуальне, ніж аналіз та оцінка функціоналу та можливостей системи на рівні ПЗ. Тому розглянемо способи захисту карт доступу докладніше.

Шифрування DES, 3DES, AESDES, 3DES, AES симетричні блокові алгоритми шифрування, де той самий ключ використовується як для шифрування, так і для дешифрування повідомлення, при чому довжина ключа залишається постійною.

DES: довжина ключа 56 біт (і 8 біт контролю парності), розмір блоку - 64 біт, був національним стандартом США (ANSI X3.92, 1977). Сучасними комп'ютерами зламується шляхом перебору за розумний час.

Triple DES (ANSI X9.52), 3DES – триразове шифрування з 3 (іноді з двома) різними ключами по 56 біт. При високому рівні захисту має досить низьку продуктивність.

AES (спочатку Rijndael, запропонований Джоан Дімен із компанії Proton World International та Вінсентом Ріджменом із бельгійського університету Katholieke Universiteit Leuven): змінна довжина ключа до 256 біт. AES - новий національний стандарт США, був обраний за результатами тестування з кількох кандидатів, оскільки поєднує простоту і високу продуктивність.

«Rijndael продемонстрував хорошу стійкість до атак на реалізацію, за яких хакер намагається декодувати зашифроване повідомлення, аналізуючи зовнішні прояви алгоритму, у тому числі рівень енергоспоживання та час виконання. Зазвичай здатність протистояти їм забезпечується за рахунок спеціального кодування для вирівнювання рівня енергоспоживання. AES можна легко захистити від таких атак, оскільки він спирається в основному на булеві операції. Крім того, чудово пройшов усі тести зі смарт-картами та в апаратних реалізаціях. Алгоритму значною мірою притаманний внутрішній паралелізм, що дозволяє легко забезпечити ефективне використання процесорних ресурсів.» – каже Річард Сміт, доктор наук, провідний інженер компанії Secure Computing Corporation.

Існують розрахунки, що показують, що для пошуку 256-бітного ключа методом повного перебору не вистачить енергії всієї нашої галактики при її оптимальному використанні. Для справжніх завдань досить 128 біт.

Використання алгоритмів шифрування DES, 3DES, AES дозволяє захистити карти доступу від несанкціонованого доступу до конфіденційних даних. [6][7][8]

Взаємна аутентифікація

За наявності алгоритму взаємної аутентифікації карта доступу, потрапляючи в зону зчитування, надає зчитувачу свій унікальний номер CSN і згенерований 16-бітний випадковий номер. У відповідь зчитувач, використовуючи алгоритм Hash, створює диверсифікаційний ключ, який повинен збігтися з ключем, записаним на карті. При збігу – карта та зчитувач обмінюються 32-бітними відгуками, після чого зчитувач «ухвалює» рішення про валідність картки. Таким чином, здійснюється захист від повторного відтворення інформації.

Диверсифікація ключа. Диверсифікація ключа необхідна в системах, де використовують карти доступу, недостатньо захищені від клонування. Як правило, це стосується низькочастотних карт стандарту Em-Marine. За допомогою ПЗ можна налаштувати розмежування доступу, що забезпечить більшу надійність СККД. [6][8][9]

Варіанти розмежування:

«карта – двері» – доступ до певних приміщень може бути дозволений лише деяким співробітникам, дані карт, яких занесено до відповідної бази даних. Тоді зловмисник із дублікатом картки доступу офісного працівника не зможе проникнути у приміщення підвищеного рівня захисту;

«карта - час» - після закінчення робочого дня, а також у вихідні та святкові дні доступ на територію підприємства та/або до комп'ютерних мереж може бути заборонено всім співробітникам;«повторний прохід» - таке розмежування не тільки не впустить у будівлю зловмисника з клоном картки вже присутнього на робочому місці співробітника, а й не дозволить самим працівникам пропускати по карті сторонніх;«вихід без входу» - за такої політики система не допустить вихід зловмисника, який увійшов без ідентифікації слідом за співробітником підприємства, але не зможе вийти клонованою карткою працівника, який уже залишив робоче місце.

Додатковий захист. Крім традиційних способів захисту карт: взаємної автентифікації пристроїв, шифрування даних та використання ключів диверсифікації, на ринку представлені рішення, що забезпечують додатковий рівень безпеки під час передачі даних від ідентифікатора до зчитувача.

Серед них слід виділити технологію Secure Identity Object™

За принципом дії картки доступу бувають контактними та безконтактними (proximity картки). Безконтактні дають більшу зручність використання (немає необхідності у прямій видимості та певному положенні карти), мають більшу відстань читання, як правило, стійкі до впливу навколишнього середовища та мають більший термін служби. Однак, у деяких випадках контактний спосіб зчитування, як і регулярна заміна карток, підвищують рівень безпеки (як приклад можна навести банківські картки).

За дальністю зчитування також знаходиться в широкому діапазоні від 0 (контактні карти доступу) до 300 метрів (активні безконтактні карти).

Залежно від технологій ідентифікації, передбачених системою, розрізняють:

- карти доступу, які використовують штрих-код;
- карти доступу, які використовують магнітну смугу;
- RIFD-картки;
- смарт-картки;
- мультитехнологічні (у тому числі біометричні) карти доступу.

Перші дві технології найчастіше використовуються як додатковий засіб захисту в комбінованих картах доступу. А технологією, що лідирує в цьому сегменті СККД, безумовно, є RIFD (Radio Frequency Identification) – радіочастотна ідентифікація.

RIFD-картки

RFID-карта по суті - носій інформації (транспондер), з якого зчитується і записується інформація за допомогою радіосигналів. Також RFID-карти називають RFID-мітками або RFID-тегами.[8]

RFID-мітки

Говорячи про радіочастотну технологію ідентифікації в системах безпеки та контролю доступу, не можна не згадати про те, що найпростіші пасивні RIFD-мітки часто застосовуються для захисту товарів від крадіжок. Для цих цілей цілком достатньо буває однобітного транспондера, який, потрапляючи в зону зчитування, сигналізує про знаходження в ній.

Крім того, різні RIFD-мітки у вигляді капсул можуть вшиватися під шкіру домашнім тваринам для ідентифікації їх у СККД.

Переваги RFID-карт

Безконтактні карти доступу на основі технології радіочастотної ідентифікації Radio Frequency Identification дозволяють швидко здійснювати доступ до системи, не вимагаючи конкретного положення мітки в просторі. Крім того, RIFD-карти дозволяють працювати в агресивному середовищі, здійснювати ідентифікацію на великій відстані та мають великий термін служби.

Завдяки використанню сучасних технологій, RIFD-карти можуть сприяти побудові систем двофакторної ідентифікації (мультитехнологічні карти доступу), а також можуть вирішувати додаткові завдання, якщо застосовується смарт-карта на основі радіочастотної ідентифікації.[6][7][8][9]

## 1.10. Класифікація RFID-карт

За джерелом живлення

RFID-карти поділяються на:

Пасивні RFID-карти. Вони так називаються через те що не мають власного джерела живлення. Працюють від електричного струму, що було індуктоване в антені карти електромагнітним сигналом зчитувача. Як наслідок мають мінімальний радіус дії, якого, втім, цілком вистачає для більшості систем. Вартість пасивних RFID-міток – мінімальна.

Активні RFID-карти мають власне джерело живлення, що дозволяє значно збільшити радіус дії, а також завдяки кращій якості передачі радіосигналу - використовувати активні RFID-мітки в більш агресивному середовищі (де для радіочастотного сигналу значно більше перешкод), наприклад, в умовах підвищеної вологості (в т.ч. у воді) або наявності у безпосередній близькості металу (автомобіль, корабель та інші металоконструкції). Проте, поліпшення технічних характеристик роботи тягне у себе збільшення розмірів RFID-карти, і навіть значне збільшення вартості.

Напівпасивні (напівактивні) RFID-карти, вони ж Battery Assisted Passive або BAP. Мають власне джерело живлення, проте його робота рідко (і лише частково) спрямована на покращення передачі радіосигналу. Радіочастотна ідентифікація, як правило, здійснюється за тим же принципом, що і пасивних RFID-картах. А енергія джерела живлення спрямована на інші

функції карти. Наприклад, живлення різних датчиків (для подальшого завантаження даних через зчитувач), забезпечення енергією систем захисту картки або живлення мікрочіпа в смарт-картках.[6]

За типом пам'яті RFID-картоки поділяються на.

- Тільки для прочитання – Read Only (RO);
- Для читання та запису даних-Read and Write (RW);

Для одноразового запису та багаторазового прочитання -Write Once Read Many (WROM).

За робочою частотою

- Найбільш поширені такі види:
- Низькочастотні proximity карти (125 кГц)
- Високочастотні RIFD-карти (13,56 МГц)
- UHF карти доступу.
- Низькочастотні proximity карти (125 кГц)

Низькочастотні RIFD-карти – Low Frequency (LF) – працюють на частоті 125 кГц. По суті, proximity карта – це дистанційна електронна перепустка, така як працює в гуртожитку КПІ або інтегрована в студентський квиток із вбудованим мікрочіпом, що має унікальний ідентифікаційний код, який широко використовується в системах контролю як фізичного, так і логічного доступу для безконтактної радіочастотної ідентифікації.

Обмін інформацією між картою та proximity зчитувачем здійснюється за відкритим протоколом, що робить проксіміті карти досить вразливими для зловмисників. Однак, низькочастотні RIFD-карти однаково ефективно працюють на відстані як з вуличними, так і з кімнатними зчитувачами; не вимагають чіткого позиціонування об'єкта і мають низьку вартість. Виготовляється такі карти доступу найчастіше у вигляді пластикової картки. Особливу популярність у СККД набули товсті карти з прорізом для власника – Clamhell.

Серед виробників proximity карт найбільш відомі: HID, Indala, EM-Marine, Ангстрем. При цьому за обсягом, який займає на ринку систем безпеки, безумовно, лідирує EM-Marine. Proximity карти Em-Marine Proximity карти Em-Marine - один із найпоширеніших форматів, що використовуються для безконтактної радіочастотної ідентифікації. Розроблено компанією EM

Microelectronic-Marin (Швейцарія, м. Марін). Ідентифікатори випускаються у формі карт, брелоків, браслетів тощо.

Proximity карти Em-Marine відносяться до пасивних розряду, т.к. не мають вбудованого джерела живлення. Перезапис карти Em-Marine не підлягає. Взаємодія між картою та proximity зчитувачем відбувається на частоті 125 кГц, радіус дії може становити від 5 до 70 см. Кожна карта має 64 біти пам'яті, 40 з них займає унікальний ідентифікаційний код

Найбільш поширені чіпи EM4100, EM4102 та TK4100.

Популярність устаткування з урахуванням формату Em-Marine пояснюється частково їх нижчою вартістю, на відміну інших стандартів (HID чи Mifare).[8]

Високочастотні RIFD-карти (13,56 МГц)

Високочастотні RIFD-карти – High Frequency (HF) – працюють на частоті 13,56 МГц. Серед виробників високочастотних карт доступу лідирують HID iCLASS SE та Seos, Mifare.

Завдяки ширшій смузі пропускання високочастотні RIFD-карти дозволяють забезпечити більший рівень безпеки та швидкодії. Карти доступу, що працюють на частоті 13,56 МГц, дозволяють реалізувати взаємну автентифікацію між карткою та зчитувачем, а також використовувати алгоритми шифрування даних.

Більшість виробників додатково чіпують високочастотні карти доступу для забезпечення додаткових можливостей і підвищення рівня безпеки. Тому високочастотні RIFD-карти часто прирівнюють до смарт-карт, що з технічної точки зору не зовсім вірно, оскільки не всяка смарт-карта працює за технологією радіочастотної ідентифікації і не всяка карта доступу з частотою 13,56 МГц може вважатися смарт-картою .

Ще однією перевагою високочастотних RIFD-карт є наявність світового стандарту ISO14443, на відміну від низькочастотних карт доступу, що не підлягають стандартизації.[8]

UHF картки доступу (860-960 МГц)

Ультрависокочастотні карти доступу - Ultra High Frequency (UHF) - працюють на частоті 860-960 МГц

Використання UHF RIFD-карток дозволяє значно збільшити відстань зчитування. Найчастіше технології UHF використовуються для організації віддаленого зчитування RIFD-міток при проїзді автотранспорту. Крім того, ультрависокочастотні карти доступу можуть застосовуватись у мультитехнологічних рішеннях для організації в'їзду на територію та входу до будівлі по одній картці."Спостерігається зростаючий попит на зчитувачі UHF з високою продуктивністю додатків, де транспортні засоби та інші об'єкти, що рухаються, повинні бути ідентифіковані автоматично за допомогою пасивних RFID-міток. Підтримка стандарту Rain RFID (UHF EPC Gen II) дозволяє компанії виробника зайняти лідируючі позиції на RFID арені" - стверджує Маартен Міджваарт, генеральний директор філії Nedap Identification Systems з Північної та Південної Америки.[6][8]

Смарт-картки доступу (smart card) або чіп-карти - являють собою пластикові картки, що мають вбудовану мікросхему, а також часто мікропроцесор та операційну систему, яка контролює пристрій та доступ до об'єктів у його пам'яті.

Види smart-карт доступу

Класифікація «інтелектуальних» карток відбувається за кількома ознаками:

1) за способом обміну даними зі зчитувачем:

контактні смарт-картки з інтерфейсом ISO7816 мають зону зіткнення з кількома невеликими пелюстками; контактні смарт-карти з USB-інтерфейсом найчастіше використовуються для аутентифікації в системі логічного доступу, взаємодіють із usb-зчитувачами; безконтактні смарт-карти, які спілкуються зі зчитувачами за допомогою RFID-технологій на частотах 125 кГц та 13,56 МГц за стандартами ISO14443 та ISO15693; зі здвоєним інтерфейсом, які працюють з різними типами зчитувачів.

2) за типом вбудованої мікросхеми: картки пам'яті, призначені лише для зберігання інформації; мікропроцесорні карти, що містять додатково програму або ОС, що дозволяє перетворювати дані за певним алгоритмом, здійснюючи захист інформації, що зберігається при її передачі, читанні, запису; карти з криптографічною логікою, що використовують алгоритми криптографування для підвищення ступеня захисту даних.

3) у сфері застосування: контроль доступу (СККД); громадський транспорт; телефонія; фінанси; банківська сфера; охорона здоров'я; програми лояльності та ін.

Переваги смарт-карт

Пластикові смарт-карти мають явні переваги в галузі захисту інформації. Питання безпеки смарт-карток регулюються багатьма міжнародними та фірмовими стандартними. Найбільш поширені:

ISO15408 - зведення правил, що стосуються безпеки цифрових систем;

Federal Information Processing Standards (FIPS) - національні стандарти США у сфері інформаційної безпеки;

FIPS-140 - вимоги до криптографічних механізмів;

EMV – спільний стандарт Europay, MasterCard та VISA для карткових платіжних систем;

Галузеві стандарти: GlobalPlatform, EPC, JavaCard і т.д.

Мультитехнологічні (комбіновані) карти доступу

Мультитехнологічні (Multi technology) карти доступу використовують відразу кілька технологій ідентифікації, за що їх часто називають комбінованими. Наприклад, мультитехнологічна карта може поєднувати кілька радіочастотних чипів; або радіочастотний чіп, магнітну смугу та контактний смарт-чіп. Насправді діапазон різних комбінацій дуже великий, тому для мультитехнологічних карт доступу немає чіткої класифікації.

Застосування комбінованих карток

Найчастіше мультитехнологічні пристрої застосовуються для поступового переходу від однієї технології до іншої: від старішої до новішої, від менш захищеної до більш захищеної. При цьому коли заміна зчитувачів більш затратна, модернізацію СККД краще почати саме з заміни карт на мультитехнологічні. Тобто одразу поміняти всі карти, які є у користувачів, на комбіновані. А зчитувачі міняти поетапно. Такий підхід дозволить уникнути великих одноразових витрат.[1][8][9]

Поки модернізація не завершиться, на об'єкті будуть працювати зчитувачі двох різних технологій. А мультитехнологічна карта потрібна, щоб

користувач міг застосовувати її для проходу точки доступу як з новими зчитувачами, так і зі старими.

Якщо ж на об'єкті, з погляду загальної вартості, більше карток – встановлюють мультитехнологічні зчитувачі, а потім уже роблять заміну карток доступу. Крім модернізації СККД, комбіновані карти можуть застосовуватися на об'єктах, які принципово використовують різні технології автентифікації для різних точок доступу. Наприклад, коли одна й та сама карта використовується для доступу на паркування (безконтактна ідентифікація з великої відстані) та до приміщень (досить звичайних proximity карт).

Мультитехнологічні (комбіновані) карти також під ходять для побудови систем двофакторної аутентифікації, проте рідко стають основою цієї системи: для покращення рівня безпеки розробники вважають за краще поєднувати карти доступу з іншими технологіями захисту. Виняток, мабуть, становлять лише біометричні карти.

Основною перевагою мультитехнологічних карт є можливість доступу через точки, що використовують різні системи аутентифікації. А у разі модернізації системи – успішний поступовий перехід із застарілих технологій без зниження поточного рівня безпеки та дискомфорту користувачів.

Сучасні біометричні карти за їх властивостями можна поділити на дві групи:

Картки з біометричними даними

Карти, що містять інформацію про біометричні дані власника: відбиток пальця, райдужна оболонка ока та/або обличчя людини – зазвичай призначені для ідентифікації особистості.

Використовуються у паспортах, візах тощо. Враховуючи стрімке зростання популярності подібних рішень з метою підвищення рівня безпеки, особливо у Європі, карти з біометричними даними збільшують власну функціональність. Наприклад, довгострокова віза, обов'язкова до отримання у Великій Британії, - Biometric Residence Permits (BRP) – є не тільки посвідченням особи, але й може бути використана як соціальна картка.

У цьому, щодо біометрії, карта є лише носієм інформації, а верифікація користувача здійснюється у разі потреби з допомогою окремих біометричних систем.

Карти з біометричною автентифікацією досить новий продукт на ринку СККД. Ця інноваційна розробка компанії Zwipe є мультитехнологічною картою, що поєднує в собі RIFD-технологію з вбудованим сканером відбитка пальця, що дозволяє реалізувати чудово захищену безконтактну карту доступу. Так, в Норвегії вже з'явилася безконтактна платіжна карта Zwipe з вбудованим датчиком відбитків пальців, розроблена за підтримки MasterCard і успішно протестована банком Sparebanken DIN.

Мультитехнологічна універсальна біометрична карти. SmartMetric випустила мультитехнологічні смарт-картки для фізичного та логічного доступу із вбудованим біометричним зчитувачем.

Для доступу до комп'ютерної мережі (логічного доступу) використовується смарт-чіп, а доступ до будівлі або приміщення (фізичний доступ) здійснюється за технологією RFID. І смарт-чіп та радіочастотна функція активуються тільки після успішної ідентифікації власника по відбитку пальця за допомогою вбудованого картки сканера. Також у карті доступу передбачені світлові індикатори, що використовуються для візуальної індикації успішного проходження біометричної ідентифікації.

Використання компанією SmartMetric супер-тонкої електроніки дозволило компанії створити карту, що має вбудований акумулятор, але при цьому не перевищує за розміром та товщиною стандартної кредитної картки.

Будова зчитувача

Спочатку розглянемо, як працює пара "карта-proximity зчитувач" (рисунок 1.6.). Зчитувач містить генератор, який запитує антену зчитувача. Енергія, що випромінюється антеною зчитувача, приймається антеною карти і використовується для живлення мікросхеми (чіп), яка при появі живлення за допомогою модулятора (М) починає модулювати сигнал зчитувача кодом, записаним в постійному запам'ятовуючому пристрої (ПЗУ) карти.[1][9][8]

Модульований сигнал у зчитувачі детектується, посилюється і надходить на мікроконтролер, який перетворює прийнятий від карти сигнал до вигляду, зручному передачі на зовнішній пристрій, до якого підключений зчитувач.

На малюнку 1.6 показано внутрішній пристрій двох типів карт: зліва карта низькочастотна (125 кГц), про що говорить антена з великою кількістю витків, а праворуч карта на 13,56 МГц з друкованою антеною.

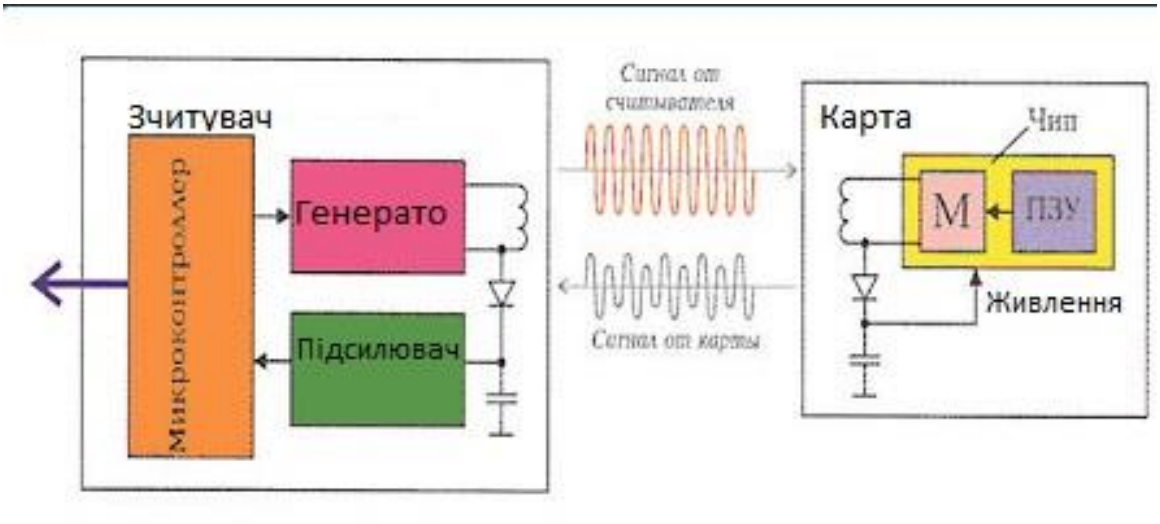


Рисунок 1.6. Принцип роботи proximity зчитувача

Порівняння інтерфейсів підключення

Усі зчитувачі підєднуються до контролеру за допомогою одного з інтерфейсів: Wiegand або OSDP.

OSDP (Open Supervised Device Protocol) – це новий сучасний протокол для обміну даними між пристроями. Може бути використаний для побудови систем контролю та управління доступом (СККД). OSDP має замінити старі протоколи обміну, наприклад Wiegand.

У чому ж основні недоліки протоколу Wiegand і в чому OSDP краще? Розглянемо їх на прикладі зчитувача карток та контролера СККД.

Моніторинг стану. При підключенні за протоколом Wiegand зчитувач не може повідомити контролера, що він несправний, оскільки однонаправлене з'єднання. Більше того, якщо є проблема у лінії зв'язку, то контролер навіть не зможе це зрозуміти. OSDP дозволяє в реальному отримувати стан лінії зв'язку і зчитувача. Таким чином підвищується надійність і знижується вартість експлуатації.

Безпека даних під час передачі. Wiegand не дозволяє шифрувати дані. OSDP у зв'язці з SCP (Secure Channel Protocol) підтримуємо взаємну автентифікацію пристроїв та передачу захищеним каналом зв'язку з шифрування AES-128.

Управління індикацією, детекторами. Так як OSDP двонаправлений протокол, то зчитувач може отримувати від контролера додаткову інформацію, наприклад, чому користувач не отримав доступу (немає права на

доступ, повторний прохід і т.д.) і виводити її на дисплей або подавати різну індикацію.

Підтримка біометрії. Раніше для використання біометричних зчитувачів або терміналів необхідна була гібридна схема підключення: біометричний зчитувач підключався до контролера протоколу Wiegand і повідомляв йому результат ідентифікації. При цьому завантаження біометричних шаблонів користувачів в зчитувач відбувалося або при підключенні до комп'ютера, або за допомогою Ethernet з'єднання. OSDP визначає варіант підключення біометричних пристроїв. Тепер з'єднання та керування здійснюється контролером безпосередньо, що, звичайно, розширює застосування біометрії в системах контролю та керування доступом.[8]

Довжина лінії до 1200 метрів. OSDP використовує стандартний промисловий протокол RS-485 як фізичний рівень. Це дозволяє підключати до пристроїв до контролера на відстані до 1200 метрів. Максимальна допустима довжина лінії при використанні протоколу Wiegand – 100 метрів.

Підтримує велику кількість пристроїв одним контролером. На одній лінії RS-485 може бути до 255 пристроїв. Пристрої можуть бути різних типів: зчитувачі, кнопки, блоки реле управління і т.д. Це дозволяє серйозно економити на монтажі та обладнанні. Наприклад, один контролер може закрити цілий поверх із великою кількістю дверей.

OSDP – це відкритий формат. Це означає, що виробники можуть додавати функції, які поки не включені до стандарту. Застосування OSDP призведе до стандартизації ринку, появи великої кількості сумісних зчитувачів і контролерів. Немає сумніву, що майбутнє за протоколом OSDP.

ІНТЕРФЕЙС «WIEGAND»

Електричне підключення. Для зв'язку між зчитувачем і контролером СККД використовується трипровідна шина - два сигнальні дроти, один загальний. На малюнку наведено класичну схему підключення, з неї очевидні й електричні параметри інтерфейсу.[6]

Максимальна довжина лінії зв'язку залежить від грамотного вибору кабелю (основні критерії — низька погонна ємність, низький омічний опір) і грамотної побудови схеми розв'язки живлення зчитувача і контролера. Звичайні значення, що наводяться постачальниками обладнання, — до 150...250 метрів.[6]

Як кабель можна використовувати кручену пару 5-ої категорії. При цьому сигнали Data0 і Data1 повинні передаватися в різних парах (провід "а"), другий провід пари (провід "б") підключається до клеми "загальний". Схема підключення до елементу живлення показана на рисунку 1.7.

Передача даних ведеться короткими імпульсами. Наявність імпульсу в лінії «Data0» означає, що був переданий лог.0, наявність імпульсу в лінії «Data1» означає, що був переданий лог.1. Ширина імпульсів та їх період сильно варіюються в залежності від виробника зчитувача. Ширина імпульсів зазвичай у діапазоні 20…200 мкс. Період проходження імпульсів - 300 ... 3000 мкс.[6]

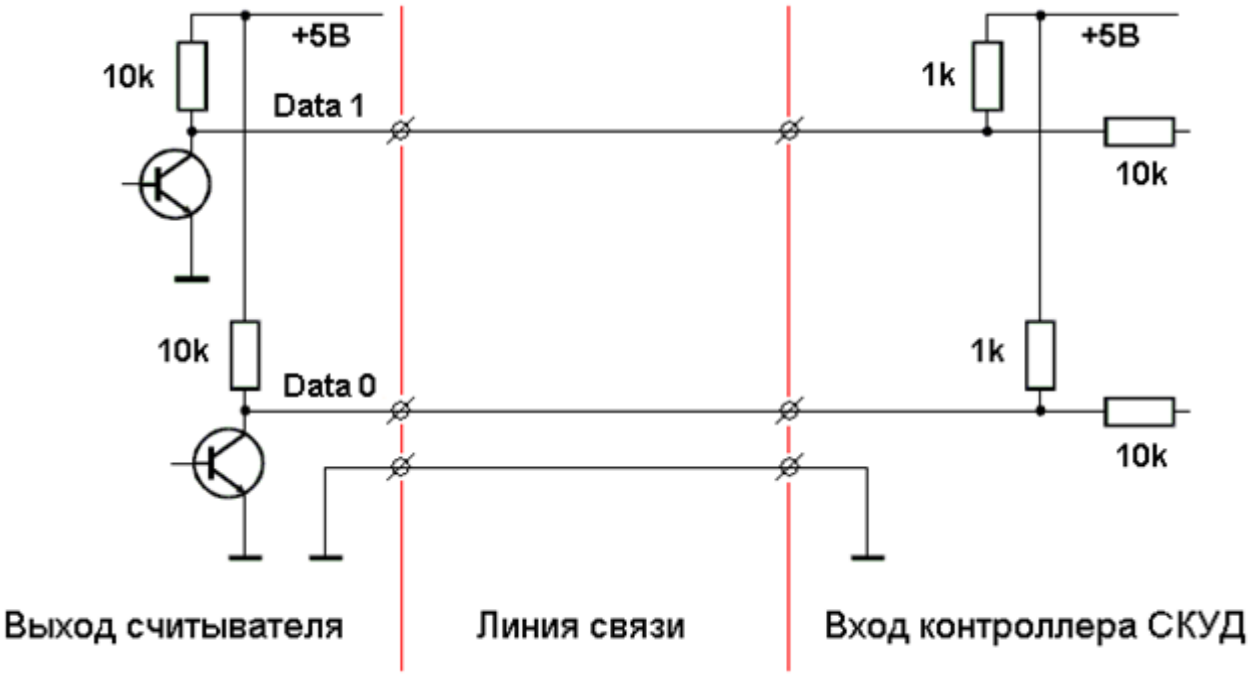


Рисунок 1.7. Схема підключення до елементу живлення.

Зв'язок односторонній, у момент виявлення карти відбувається одноразова передача кадру з кодом картки від зчитувача до контролера СККД. Передача йде старшим бітом коду вперед.[6]

Поділ кадрів здійснюється за тайм-аутом. Реально мінімальний час між кадрами 0,5 сек., що рекомендується тайм-аут для контролера СККД - 50 ... 250мс.

Історично склалося так що багато систем контролю доступу та виробники карток умовно ділять код карти на дві нерівні частини, які

називають фасиліті та номер. Зазвичай до номера відносять молодші 16 біт коду, все інше фасиліті. Причина такого поділу — економія пам'яті в старих контролерах доступу. При монтажі об'єкта підбиралися карти з однаковим фасилітом і в пам'ять контролера записувалися лише молодші 16 біт коду мітки (номер). З того часу пройшло багато часу і подібна економія давно в минулому, але багато систем все ще оперують цими поняттями, показуючи код карти розділеним на частини. В наш час жодного смислового навантаження такий поділ не має.[6]

Якщо є контроль за парністю, то до біт коду карти додаються два біти - один перед кодом, інший після. Відповідно, весь код карти ділиться рівно посередині на дві частини. парність старшої половини коду контролюється першим бітом, молодшою - останнім. Якщо кількість біт у коді непарна, то центральний біт коду входить в обидва контрольні парності.

Перший біт парності (старшої половини коду) ставиться в 1 якщо кількість одиниць у половині коду непарне. Останній біт парності (молодшої половини коду) ставиться в 1 кількість одиниць у його половині коду парне.

Слід зазначити, що зустрічаються зчитувачі не підкоряються цьому правил контролю парності. Тому реально більшість універсальних контролерів СККД просто ігнорують контроль на парність. Крім того, деякі формати безконтактних карт несуть інформацію про кількість біт коду та парності прямо на карті, відповідно зчитувач не може жодним чином впливати на реальний вихідний формат даних. Такий, наприклад, формат HID ProxPass, Indala ASP та ін.

Wiegand та клавіатури для введення PIN коду

Багато СККД підтримують ідентифікацію за набором PIN-коду на клавіатурі. При цьому набраний код може бути як основною ідентифікаційною ознакою, так і додатковою. Зазвичай набраний код також передається по інтерфейсу Wiegand. Існують різні підходи до його передачі, найбільш поширені такі:

Wiegand-26. При цьому цифри, що вводяться, буферизується на зчитувачі, а по закінченні набору передаються всі разом у складі однієї Wiegand посилки. Спосіб кодування цифр у посилку не стандартизований, але найчастіше це кодування BCD, що дозволяє передати код довжиною до 6 цифр (6=24/4).[6]

Wiegand-4, Wiegand-6, Wiegand-8. При цьому цифри, що вводяться, відправляються по Wiegand окремо в міру введення. Загальноприйнятого стандарту кодування цифр у посилку немає, але найпоширеніші варіації, які називаються Wiegand-HID (Wiegand-6) і Wiegand-Motorola (Wiegand-8).

В обох підходах крім цифр як таких часто зчитувачі можуть передавати по Wiegand службові символи, такі як # і *, якщо вони присутні на клавіатурі.[6]

## 1.11. Протипожежна система

Датчики диму

Датчики диму поділяються на:

- Іонізаційні
- Оптичні
- Аспіраційні
- Лінійні
- Іонізаційні пожежні сповіщувачі

Іонізаційний пожежний сповіщувач – це високотехнологічний автоматичний пристрій для реєстрації вогнища пожежі за появою в газоповітряному середовищі приміщення летких продуктів, що захищається, процесу горіння – дрібних частинок кіптяви, гару. Такий спосіб виявлення заснований на властивості іонізованого повітря притягувати частки димового потоку, що і послужило появі такої назви.[2][3]

Сповіщувач пожежний димовий

За своєю ефективністю, це одна з останніх щаблів технічного розвитку димових пожежних сповіщувачів, порівнянна за чутливістю, швидкістю/інерційністю виявлення характерних ознак процесу горіння з утворенням димів лише з газовими, аспіраційними, проточними датчиками; перевищуючи показники оптико-електронних пристроїв, призначених для таких же цілей.

Іонізаційні пожежні сповіщувачі здатні виявляти вогнище займання не тільки на ранній стадії по появі летких частинок реакції горіння, але і реагують на будь-який їх розмір; а також колір, що залежить від фізико-хімічних

параметрів пожежного навантаження в приміщеннях, що захищаються, так званий сірий і чорний дим; що недоступно для більшості інших автоматичних пристроїв, що фіксують утворення димового потоку.

Через складність виробництва, технічний контроль при створенні подібних пристроїв; необхідності утилізації/дезактивації, що відслужили свій термін іонізаційних пожежних сповіщувачів тільки на спеціалізованих підприємствах атомної промисловості, створено передумови високої вартості виробів.

У силу наявності в них, нехай і в допустимих державними нормами, невеликої кількості радіоактивних речовин усередині мініатюрних радіоізотопних випромінювачів, що є невід'ємним елементом конструкції більшості моделей виробів; частково через сформовану упереджену громадську думку в нашій країні вони серійно не виробляються.

Однак, за кордоном їх виготовлення триває, і сертифіковані в установленому порядку вироби можна придбати на ринку пожежно-технічної продукції.

Згідно з визначенням, даним у ГОСТ Р 53325-2012, це автоматичний пристрій виявлення вогнища займання, спосіб дії якого ґрунтується на зміні значень електричного струму, що проходить через штучно іонізоване повітря, при появі в них димових частинок, що утворилися в процесі горіння твердих рідких матеріалів.[2][3]

За контрольованою ознакою пожежі, конструкції виробів, технічного пристрою чутливих елементів датчиків, способу виявлення димових частинок

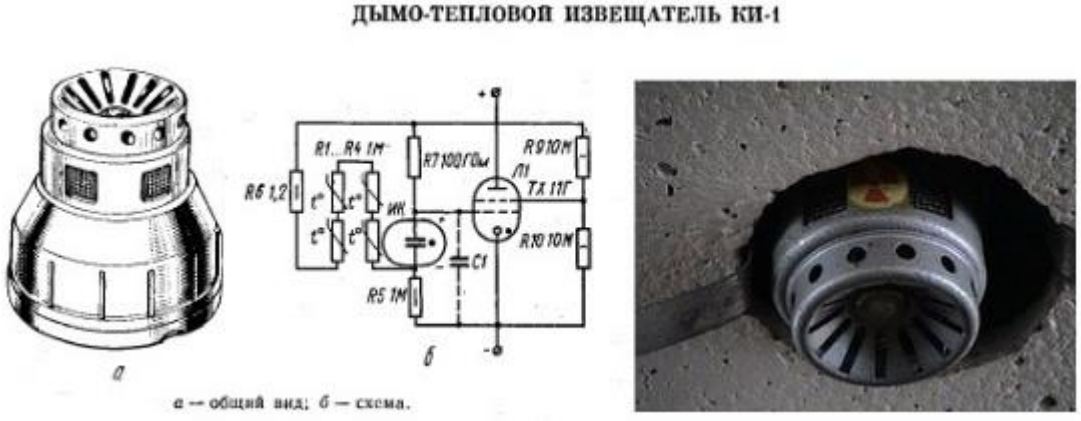


Рисунок 1.8. Димо-тепловий сповіщувач

Радіоізотопні сповіщувачі

Це пожежний димовий сповіщувач, який спрацьовує через вплив продуктів згоряння на струм іонізації внутрішньої робочої камери сповіщувача. Принцип дії радіоізотопного детектора заснований на іонізації повітря приміщення при опроміненні радіоактивною речовиною. Принцип дії радіоізотопного детектора заснований на іонізації повітря приміщення при опроміненні радіоактивною речовиною. При введенні протилежно зарядженого електрода в камеру виникає струм іонізації. Заряджені частинки «прилипають» до більш важких частинок диму, знижуючи їх рухливість – знижується іонізаційний струм. Зниження його до певного значення сповіщувач сприймає як «тривожний» сигнал. Іонізаційні пожежні сповіщувачі.

Аерозольні частинки засмоктуються з навколишнього середовища в циліндричну трубку (газохід) за допомогою малогабаритного електричного насоса та потрапляють у зарядну камеру. Під впливом уніполярного коронного розряду, частинки набувають об'ємний електричний заряд і, рухаючись далі газоходом, потрапляють у вимірювальну камеру, де наводять на її вимірювальному електроді електричний сигнал, пропорційний об'ємному заряду частинок і, отже, їх концентрації. Сигнал з вимірювальної камери потрапляє в попередній підсилювач і далі блок обробки і порівняння сигналу. Датчик здійснює селекцію сигналу за швидкістю, амплітудою та тривалістю і видає інформацію при перевищенні заданих порогів у вигляді замикання контактного реле. На рисунку 1.9 зображено структурну схему електроіндукційного сповіщувача.[2][3]

1. Високовольтний модулятор.
2. Регулятор напруги.
3. Блок живлення.
4. Підсилювач.
5. Блок обробки інформації
6. Зарядна камера, кільце електрод.
7. Зарядна камера, електрод голка.
8. Конденсатор.
9. Резистор.
10. Резистор.
11. Стабілітрон.
12. Індукційний електрод.
13. Світлодіод.
14. Підприємець витрати аерозолю.

15.F – Вихідний сигнал.

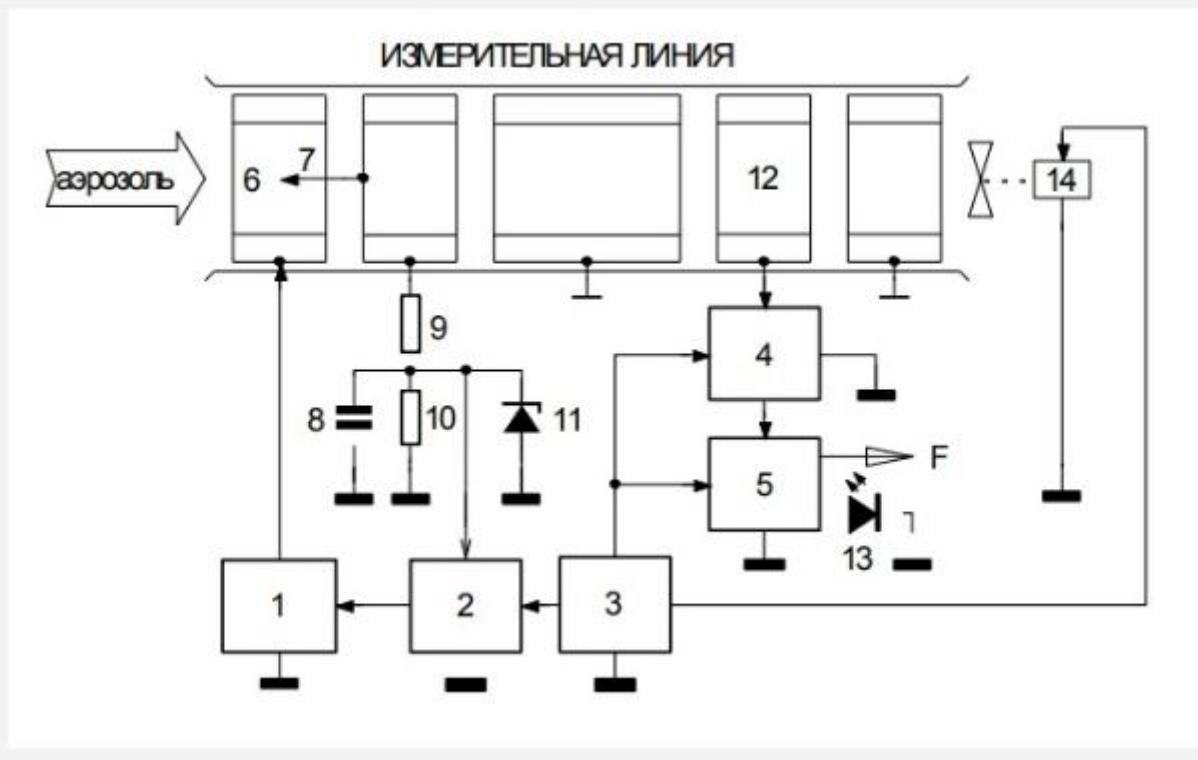


Рисунок 1.9. Структурна схема електроіндукційного пожежного сповіщувача

Принцип дії грунтується на фіксації, реєстрації змін показників електроструму, що проходить через іонізовані молекули повітряного середовища в чутливому елементі датчика, при впливі на них дрібних частинок летких продуктів реакції горіння.

При попаданні таких частинок в камеру датчика іонізаційного димового сповіщувача вони за рахунок різниці електричних потенціалів приєднуються до іонів, що знижує швидкість їхнього руху і, як наслідок, силу струму; при зниженні їх кількості, видаленні з чутливого елемента пристрою сила струму починає зростати.

Зменшення сили електроструму, що проходить через іонізоване повітря, до порогового/критичного значення, встановленого налаштуваннями виробу, сприймається пристроєм як ознака виявлення вогнища пожежі в приміщенні, що контролюється зоні; з формуванням, передачею тривожного повідомлення на приймально-контрольну апаратуру установки АПС чи блок управління системи автоматичного пожежогасіння.

Принцип роботи радіоізотопних димових сповіщувачів ґрунтується на іонізації повітряного середовища в контрольній камері чутливого елемента, розміщеного всередині корпусу виробу, при інтенсивному випромінюванні його малопотужним вузькоспрямованим джерелом радіоактивного випромінювання; в електроіндукційних пожежних датчиках іонізація повітря здійснюється коронним уніполярним розрядом електричного струму.

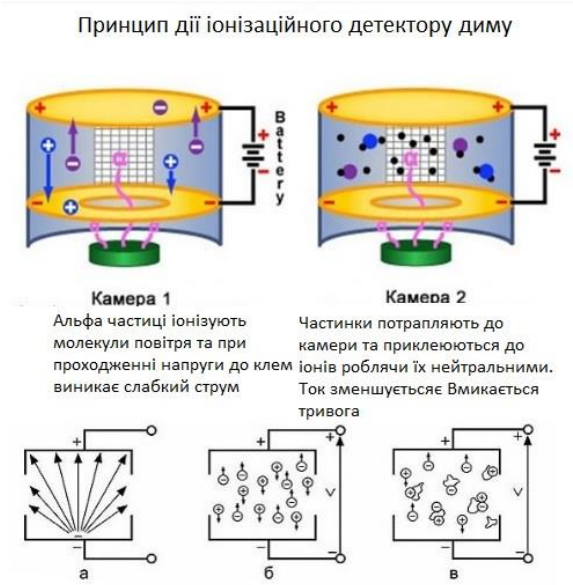


Рисунок 1.10. Принцип дії іонізаційного детектору диму.

Оптико-електронний лінійний пожежний сповіщувач

Це двокомпонентний пристрій, що складається з приймача та випромінювача або єдиного блоку випромінювача/приймача, що реагує на появу димових газів між ними або блоком універсального датчика та відбивачем.

По ГОСТ 53325-2012 лінійний оптико-електронний сповіщувач – це пожежний датчик, який формує оптичний промінь, що пронизує контрольовану зону газоповітряного середовища приміщення поза пристроєм, що визначає характерну ознаку пожежі щодо ослаблення інтенсивності променя у разі задимлення.

Крім того, в цьому документі наведено такі визначення:

Передавач – блок сповіщувача, що генерує оптичне випромінювання.

Відбивач – елемент лінійного димового сповіщувача, який служить для зміни напрямку оптичного променя, що генерується передавачем.

Оптична довжина – найкоротша відстань, якою йде промінь від передавача до приймача.

Приймач лінійного димового сповіщувача - це універсальний пристрій, що об'єднує в одному корпусі вироби обидва елементи.

Випромінювач/приймач, блок приймача жорстко, нерухомо встановлюють на стінах, стовпах, колонах, перегородках так, щоб вісь оптичного променя проходила на відстані не менше 0,1 м, не більше 0,6 м від нижньої точки конструкції перекриття; а допустимі відстані між ними, як і, як і ширина контрольованої зони, визначається кожного конкретного вироби, за даними технічного паспорта.

Димовий оптико-електронний аналоговий

Це датчик диму, який відрізняється від порогових моделей виробів, тим що він фіксує не досягнення критичного значення щільності газоповітряного середовища в приміщенні, що захищається, а її зміни в реальному часі; що набагато ефективніше для раннього виявлення вогнища займання по появі летких газоподібних, аерозольних сумішей в результаті піролізу, тління твердих матеріалів у пожежному навантаженні.[2][3]

Адресно-аналоговий оптико-електронний димовий

Це один із найновіших пристроїв для ефективного виявлення найменших ознак появи летких продуктів горіння в контрольованій зоні.

Насправді, він є комбінованим димовим пожежним сповіщувачем, т.к. визначає характерні ознаки вогнища горіння не тільки щодо досягнення порового значення падіння оптичної щільності повітря в приміщенні, але й за його диференційною зміною за встановлений налаштуваннями період; що набагато надійніше, адже контроль здійснюється відразу за двома параметрами.[2][3]

Димовий оптико-електронний адресно-аналоговий сповіщувач

Це прилад живиться за шлейфом установки АПС і має вбудований звуковий пожежний оповіщувач, рекомендований СП 5.13130 для застосування як технічний засіб як для точного визначення місця виникнення вогнища загоряння за появою диму, так для локального оперативного оповіщення людей, що знаходяться в громадських будинках, включаючи експозиційні зали музеїв, картинних галерей, читальні зали бібліотек, об'єкт

торгівлі; а також для встановлення у приміщеннях цехів промпідприємств, складів із постійним, змінним знаходженням працівників.

Використання димових оптико-електронних адресно-аналогових сповіщувачів із вбудованим звуковим сповіщувачем про пожежу у складі установок АПС, автоматичного пожежогасіння не означає можливості не проектувати, монтувати системи для оперативного оповіщення людей, які перебувають у будинках на момент виникнення надзвичайної ситуації.

Димовий оптико-електронний пожежний сповіщувач

Це прилад, який за допомогою чутливого елемента датчика визначає появу вогнища, в т.ч. процес піролізу, тління, утворення димових газів на ранніх стадіях розвитку, набагато раніше як максимальних, так і диференціальних, максимально-диференціальних теплових пристроїв.

Саме з цим пов'язане пояснення нормативних вимог щодо необхідності встановлення димових ІП на об'єктах із масовим перебуванням людей – у торговельно-розважальних, музейно-виставкових, адміністративних, ділових центрах; навчальних закладах будь-якого рівня освіти – від дитячих садків до університетів; спортивні споруди, розважальні установи; а також для захисту всіх об'єктів незалежно від функціонального призначення, кількості відвідувачів, працівників, де пожежне навантаження у приміщеннях у разі виникнення вогнищ загорянь схильна до димоутворення.

Найбільшого поширення при проектуванні, створенні схем/структур автоматичних установок АПС, систем пожежогасіння різних об'єктів захисту набули оптико-електронні точкові датчики диму, які за ГОСТ Р 53325-2012 здатні поглинати, відбивати або розсіювати оптичне випромінювання в невеликому обсязі; набагато менше, ніж весь простір приміщення, що захищається.Іншими словами, точковий оптико-електронний датчик диму реагує на ознаки/фактори появи вогнища займання в компактній, обмеженій як його технічними можливостями, так і висотою установки на стелі, під перекриттям приміщень об'єкта, що захищається. Так, за табл. 13.3* СП 5.13130.2009, площа, контрольована точкові м димовим датчиком, що не перевищує 85 м2 при висоті установки 3, 5 м.

Принцип дії, маркування, конструкція

Принцип дії точкових оптико-електронних датчиків ґрунтується на здатності інфрачервоного випромінювання розсіювати так званий сірий дим, що виділяє при горінні більшості твердих матеріалів. У той же час вони, на

відміну від іонізаційних пожежних сповіщувачів, практично не реагують на «чорний» дим, що утворюється під час горіння важких нафтопродуктів, багатьох полімерів, пластиків/пластмас, іншої продукції підприємств органічного синтезу.

Конструкція будь-якого точкового димового датчика передбачає наявність роз'ємної основи з чотирма контактами/клемами, що кріпиться до стелі, що найчастіше називається монтажною розеткою, необхідної як для зручності, швидкості установки сповіщувача, контролю його працездатності; так і для спрощення регламентних процедур під час проведення регулярного технічного сервісу з перевірки, очищення, налаштування за необхідності цих пристроїв виявлення можливих вогнищ пожежі.

Точкові оптико-електронні датчики диму, марковані НПБ 76-98 абревіатурою ІП 212-ХХ, застосовують для виявлення ознаки займання ефект розсіювання променя світлодіода у складі конструкції на дрібних димових частинках, що потрапили у вимірювальну камеру датчика.[2][3]

**Висновки до розділу 1**

В даному розділі було розглянуті існуючі системи безпеки, структурну будову існуючих систем, їх складові. Розглянули конструкцію більшості сповіщувачів. В усіх місцях де може бути встановлена система безпеки вона повинна буде встановлена.

## 2. Проектування системи безпеки

Система безпеки побудована на базі програмно-технічного комплексу від фірми Bosch – Bosch Security System. Ядром якої є програмне забезпечення Building integrates system до якої входять компоненти Access engine, який відповідає за доступ до певної зони охорони, контроль працівників, часові моделі зон охорони. Security Engine відповідальне за опис події на, дату та час події, місце де виникла неочікувана подія, адреса панелі або сповіщувача що створив сигнал події. Та Video Engine яке відповідає за відеоспостереження. Усі програми знаходяться на сервері який встановлюється в найбезпечніше місце для запобігання фізичного втручання в його роботу. Оператори користуються клієнтськими версіями програмного забезпечення. Структурна схема безпеки приведена в додатку А. Розміщення усіх приладів зображено в додатку Б.

Серцем системи є головна панель ICP-MAP5000-2. Панель ICP-MAP5000-2 зображена на рисунку 2.1. Позначення клем та портів підключення зображено на рисунку 2.2.

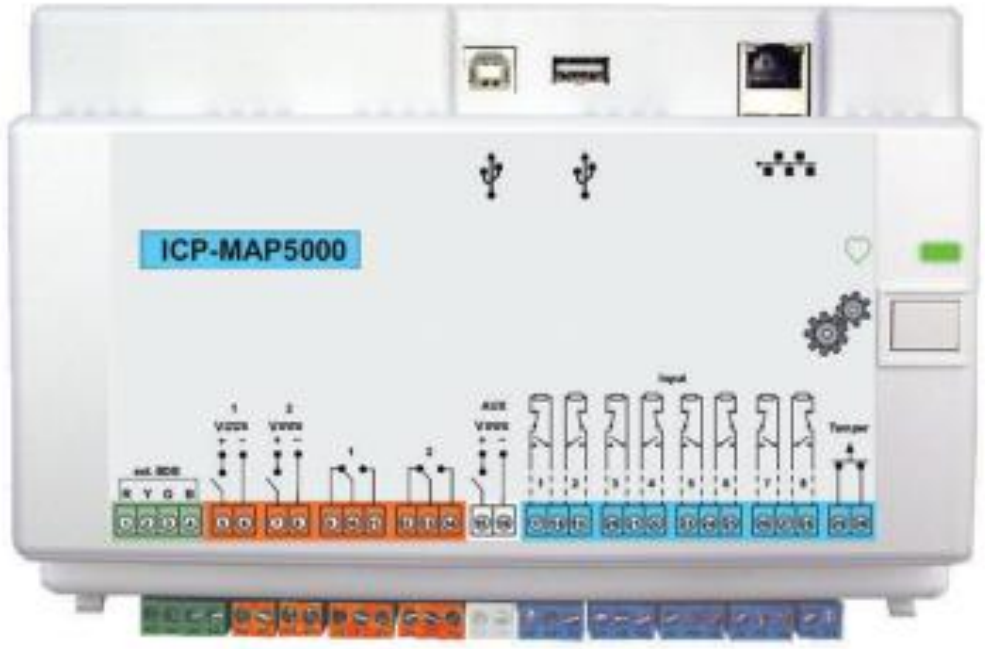


Рисунок 2.1 Головна панель ICP-MAP5000-2

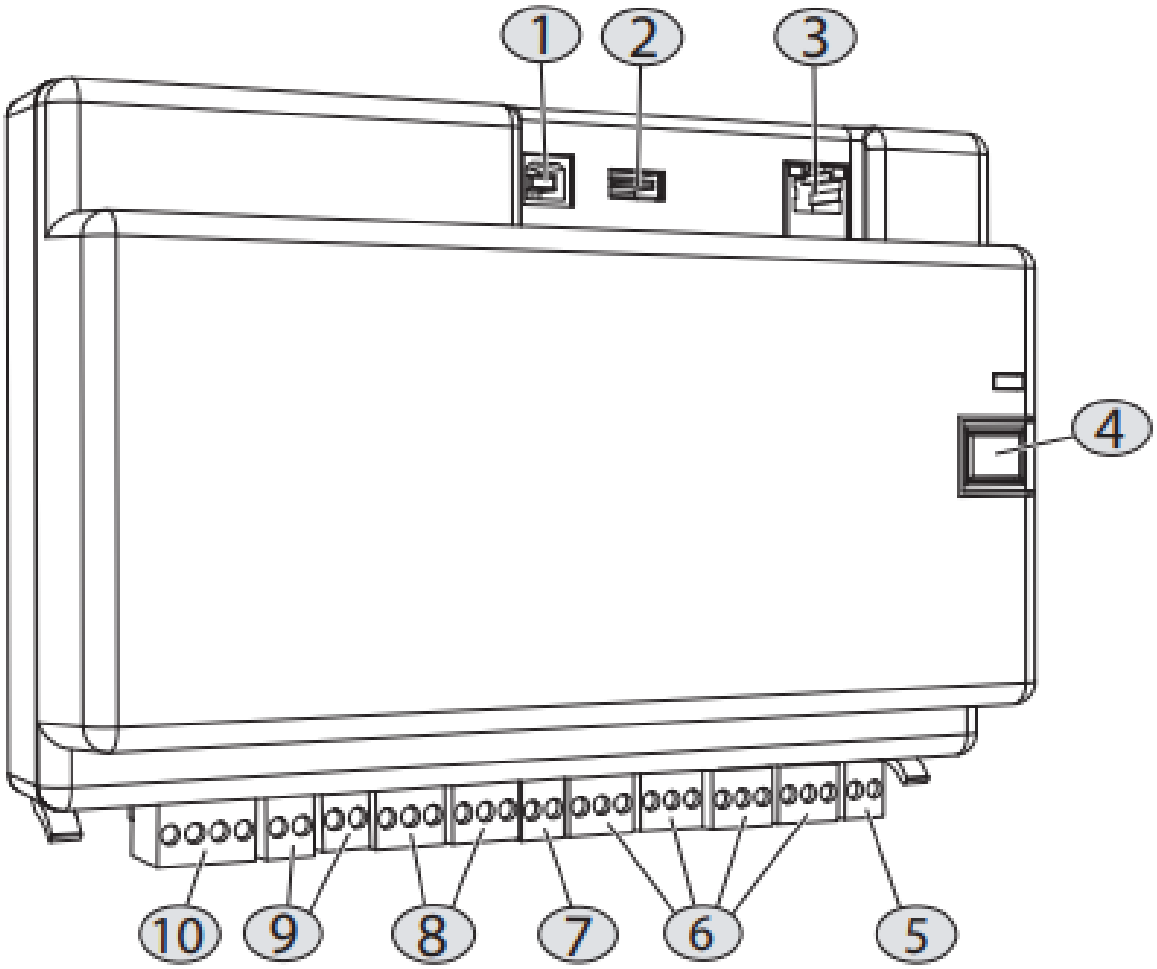


Рисунок 2.2 Позначення клем та портів підключення

| Елемент | Опис |
|---|---|
| 1 | Порт USB-хост: в даний час не діє |
| 2 | Порт USB-хост: в даний час не діє |
| 3 | Порт Ethernet |
| 4 | Кнопка установщика |
| 5 | Вхід контакта несанкціонованого закріплення |
| 6 | Восемь входів з контролем лінії |
| 7 | Виход вспомогательного харчування |
| 8 | Два релейних вихід типу С із сухими релейними |

| | |
|---|---|
| | контактами |
| 9 | Два вспомогательных керованих виходу с напругм |
| 10 | Порт зовнішньої шини даних Bosch (BDB) |

Зовнішня шина BDB загальною довжиною до 1000 м дозволяє розміщувати пульти управління, шлюзи LSN, розгалужувачі CAN та блоки живлення у місцях використання, сприяючи більшій ефективності.

Електричні характеристики

| | |
|---|---|
| Мінімальне робоча напруга, постійний струм, В | 19 |
| Максимальне робоче напруга, пост. струм, В | 29 |
| Номінальна напруга, пост. струму | 28 |
| Мінімальне споживання струму, мА | 250 |
| Максимальне споживання струму, мА | 500 |
| Вихідні характеристики | |
| Максимальне споживання струму, мА на вихід | 1000 |

LSN модуль підключається кільцевим шлейфом зовнішньої шини даних Bosch до MAP. Кільцеве з`єднання дає системі можливість функіонувати без перебоїв через те що при вилученні одного з модулів система буде передавати інформацію до центральної панелі по шині типу промень, таким чином створюється два промені та система працює без перебоїв.[10]

До кожного модуля LSN можна підключити один кільцевий або два радіальні шлейфи LSN зі струмом навантаження трохи більше 300 мА. Кожен модуль LSN підтримує до 127 пристроїв LSN. Модульна охоронна платформа MAP 5000 підтримує до восьми модулів LSN на внутрішній та зовнішній шинах передачі даних Bosch (BDB) та до 1500 адрес. Позначення клем та портів підключення зображено на рисунку 2.3.

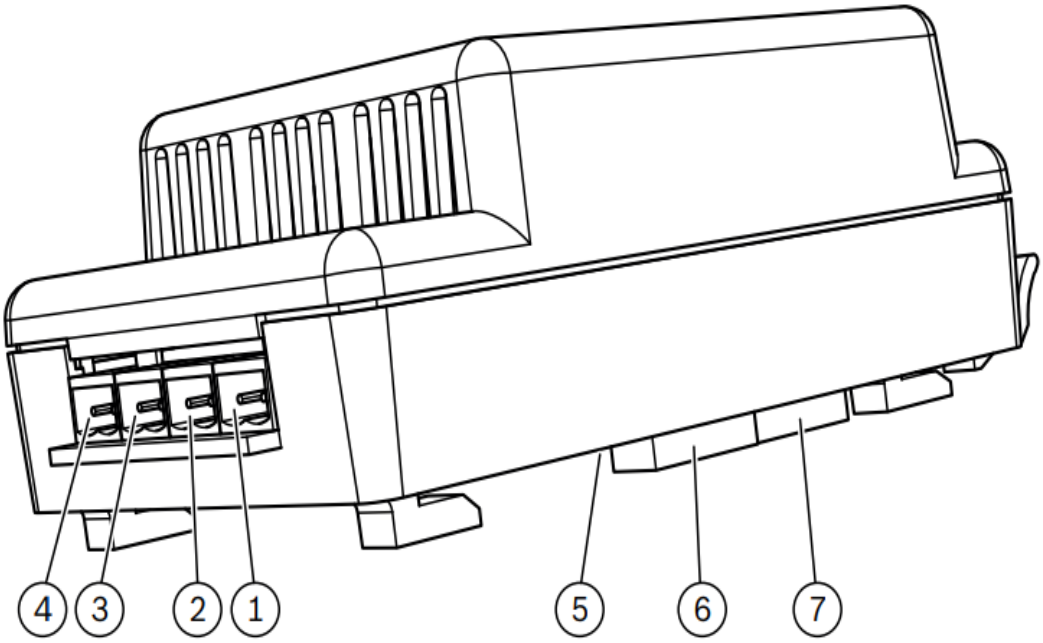


Рисунок 2.3. Позначення клем та портів підключення

Позначення елементів

| Елемент | Опис |
|---|---|
| 1 | LSN1: допоміжне живлення |
| 2 | LSN1: шина даних LSN |
| 3 | LSN2: допоміжне живлення |
| 4 | LSN2: шина даних LSN |
| 5 | Вхід контакту несанкціонованого розтину пристрої: в даний час не використовується |
| 6 | Роз'єм шини даних Bosch (B) |

7 Роз'єм шини даних Bosch (A)

Електричні характеристики

| | |
|---|---|
| Мінімальне робоча напруга, пост. струм | 16 |
| Максимальна робоча напруга, пост. струм | 29 |
| Номінальна напруга В, пост. струму | 28 |
| Максимальний струм, мА | 1500 |
| Номінальний струм у мА | 75 |
| Максимальний струм лінії LSN, мА | 300 |
| Максимальний струм на виході допоміжного живлення LSN, мА | 2*500 |

Для включення сповіщувачів в систему використовується модуль розширення LSN. ISP-EMIL-120. Контакти підключення зображено на рисунку 2.4.[10]

| | |
|---|---|
| PL1-PL6 | Шлейфи |
| S1-S4 | Керуючі виходи |
| SP | Вільні клеми, наприклад для підключення резисторів в шлейфах |
| WT | Тампер |

Шлейфи PL 1 – PL 6

• Шлейфи PL 1 – 6 використовуються для підключення неадресних сповіщувачів, наприклад контактних сповіщувачів, магнітних контактів та ригельних контактів. Сповіщувачі, підключені до шлейфу, групуються в одну зону сповіщувачів.

• Зони сповіщувачів можуть бути запрограмовані як тривожна кнопка, проникнення, розтин корпуси, ригель-контакт чи вхід. Аналіз повідомлення програмується на контрольній панелі.

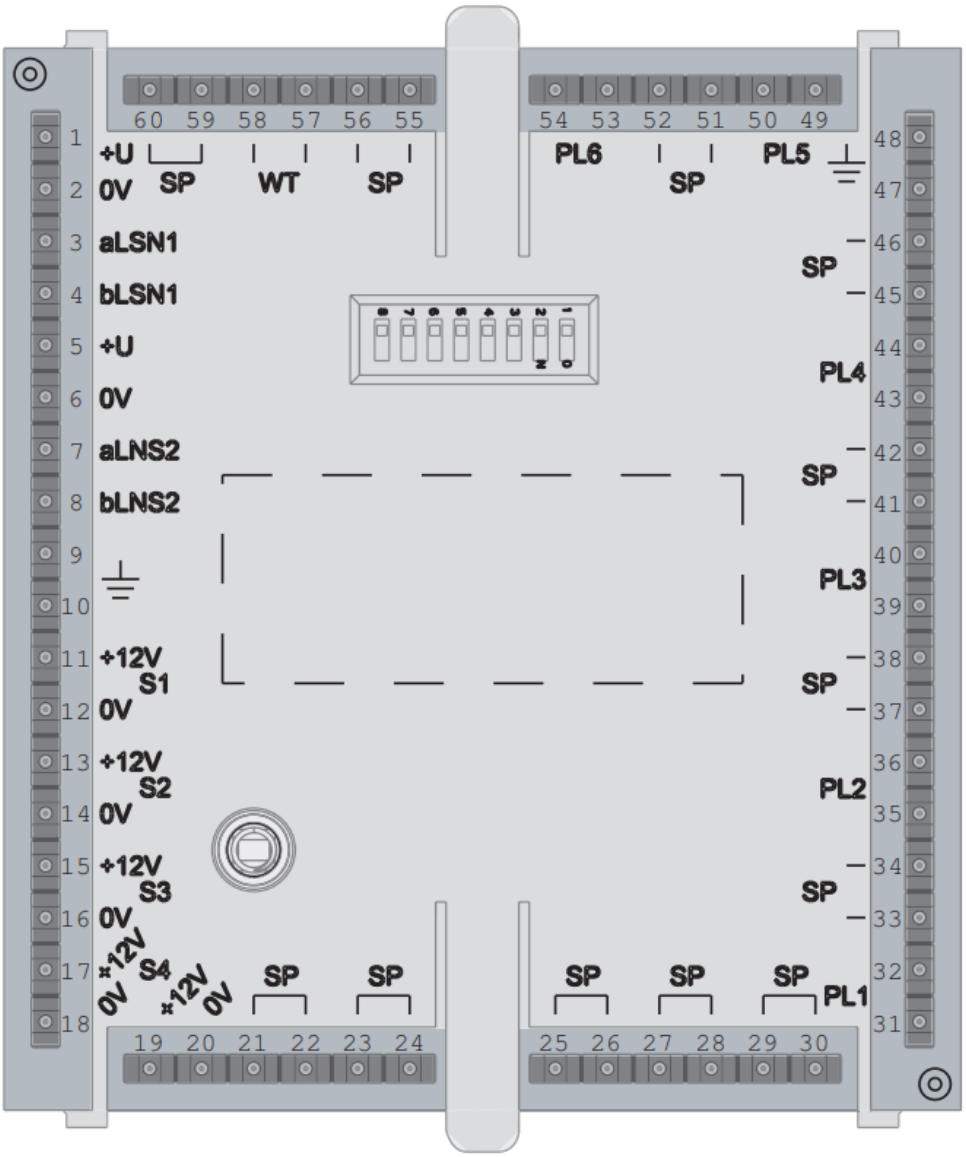


Рисунок 2.4. Контакти Emil модуля.

Шлейфи PL 1 – PL 6

Шлейфи PL 1 – 6 використовуються для підключення неадресних сповіщувачів, наприклад контактних сповіщувачів, магнітних контактів та ригельних контактів. Сповіщувачі, підключені до шлейфу, групуються в одну зону сповіщувачів.

Зони сповіщувачів можуть бути запрограмовані як тривожна кнопка, проникнення, розтин корпуси, ригель-контакт чи вхід. Аналіз повідомлення програмується на контрольній панелі.

Шлейфи PL 5 – 6 можуть використовуватись для підключення сповіщених по шлейфу сповіщувачів розбиття скла.

Керуючі виходи S1 – S4

Є 4 керуючі виходи, використання та управління якими залежить від підключених сповіщувачів.

В адресних шлейфах функції виявлення та управління виконуються з використанням лінії LSN. Це означає, що немає необхідності в додаткових шлейфів у контрольній панелі для виконання керуючих функцій. Невикористовувані керуючі виходи можуть бути вільно запрограмовані на виконання функцій панелі.

Зони охорони території промислового центру по виготовленні сиру зображено на рисунку 2.5.

На зонах 1-4 подібний набір систем. На зоні 5 знаходиться лише пожежні сповіщувачі та периметральні датчики та ДРС встановлені на КПП1 та КПП2. Зона 1 також відрізняється наявністю ДРС.[9][10]

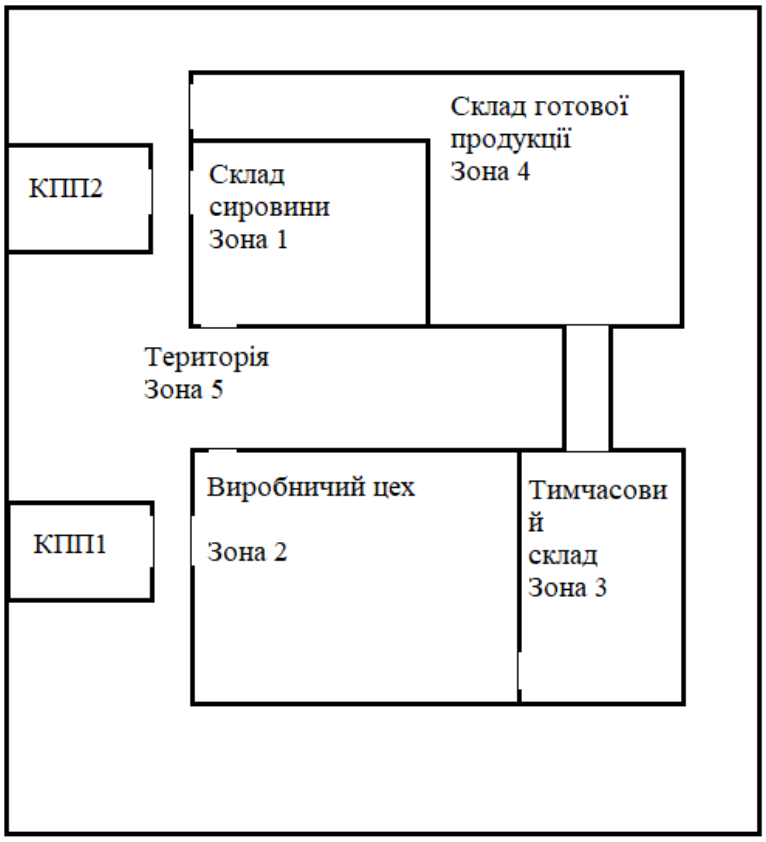


Рисунок 2.5. Схема розміщення зон безпеки на виробництві.

## 2.1. Сповіщувачі встановлені в зонах 1-4

Датчики розбиття скла встановлені в зонах 1 та 5. Для встановлення були обрані ДРС DS1101i.

Рисунок 2.6 Датчик розбиття скла

Технічна специфікація

| | |
|---|---|
| Зона сприйняття | 7.6м |
| Струм | 23мА при 12 В пост. струму |
| Напруга | 6-15 В пост. струму |
| Умови експлуатації | |
| Робоча температура | -29 - +50°C |

Пожежний сповіщувач AVENAR detector 4000 розташований в зонах 1-4.

Рисунок 2.7. Пожежний сповіщувач

Цей сповіщувач поєднує оптичний сенсор(диму), тепловий сенсор (датчик температури), хімічний сенсор. Він поєднує в собі усі сенсори що входять до спектру пожежних систем.

Оптичний сенсор (димовий)

У роботі оптичного сенсора застосовується принцип виміру розсіяного світла. Світлодіод випромінює світло у вимірювальну камеру, де він поглинається складною структурою лабіринту. У разі виникнення пожежі дим потрапляє у вимірювальну камеру, та частинки диму розсіюють світлодіод. Кількість світла, що потрапляє на фотодіод, перетворюється.

Тепловий сенсор (датчик температури)

Термістор в ланцюжку опорів використовується в як тепловий сенсор, від якого аналогоцифровий перетворювач через задані тимчасові інтервали отримує залежне від температуру напруги.

Хімічний сенсор (газовий)

Основна функція газового сенсора полягає в виявленні чадного газу (CO), що є продуктом горіння, але він також виявляє водень (H) та моноксид азоту (NO). Значення сигналу сенсора пропорційно концентрації газу. Газовий сенсор надає додаткову інформацію для ефективного придушення зовнішніх впливів. В даній системі даний датчик доповнює кліматичний датчик BME680. Для виготовлення сиру слідкування за кліматичними параметрами такими як вологість, температура, аналізатор повітря. Кліматичний датчик BME680 зображено на рисунку 2.8. 4 такі датчики розташовані в зонах 1-4.[10]

Датчик температури дозволяє вимірювати температуру у всьому робочому діапазоні -40 ... +85 °C. Абсолютна точність у діапазоні 0 …+65 °C становить ±1 °C.

Датчик тиску має робочий діапазон 300...1100 кПа з роздільною здатністю 0,18 Па. У діапазоні температур 0…+65 °C сенсор характеризується абсолютною похибкою ±0,6 кПа.

Датчик вологості працює в діапазоні 0…100% з абсолютною точністю ±3% (температура 0…+65 °C).[10]

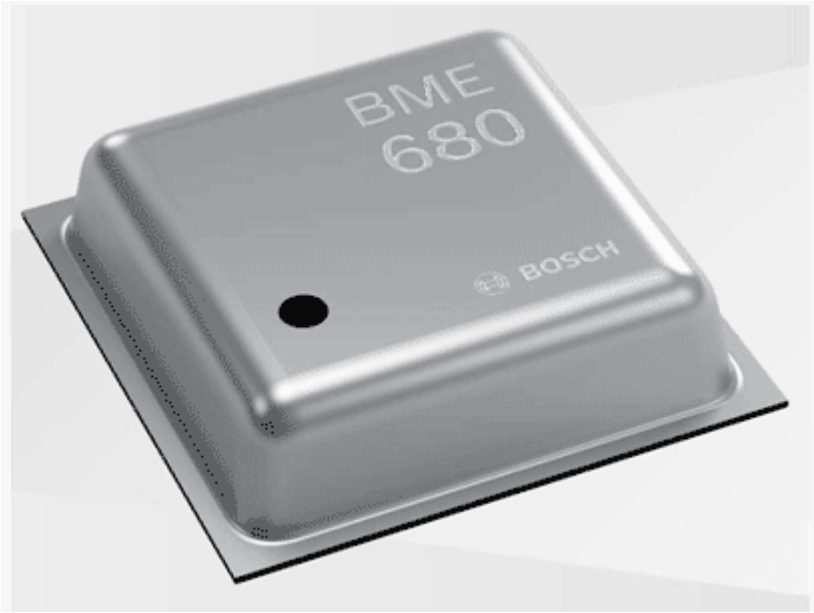


Рисунок 2.8. Кліматичний датчик BME680

## 2.2. Система керування доступом

Проміжною одиницею в системі керуванням доступу є контролер доступу AMC2 4W. Зовнішній вигляд показано на рисунку 2.9. До контролеру підключаються зчитувачі карт та геркони (датчики відчинення дверей), електроні замки. Верхня частина плати зображена на рисунку 2.10. Нижня частина плати зображена на рисунку 2.11. Пункти 16 та 17 працюють в парі. Використовуючі інтерфейс Wiegand підключаємо зчитувачі. До виходів 17 підключаються геркони. 18 виходи відповідають за підключення електричних замків.


Рисунок 2.9. Контролер доступу AMC2 4W.

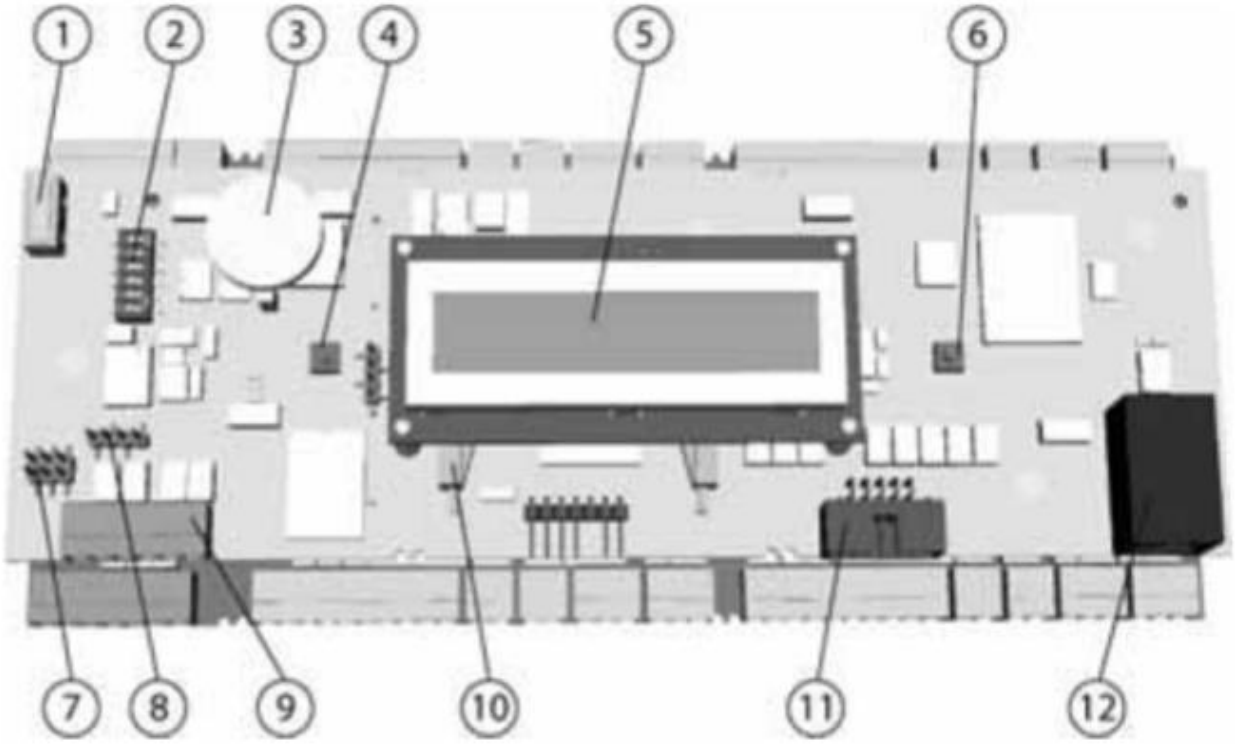


Рисунок 2.10. Верхня частина плати AMC2 4W

1 Внутрішній контакт тампера

2 DIL перемикач для вибору адреси RS-485, протоколу та вибору RS-232/RS-485

3 Литієвий акумулятор для буферизації статичної RAM та real time clock (RTC)

4 Кнопка скидання до почтакових налаштувань

5 Дисплей

6 Режим відображення

7 Перемичка: вирівнювання потенціалу між різними системами та заземленням (екран)

8 еремичка: вибір інтерфейсу RS-485 Підключення до головному комп'ютеру, RS-485 двопровідне або RS-485

9 Інтерфейс RS-485 головного комп'ютера, що настроюється.

10 Порт для картки пам'яті Compact Flash

11 Настроюваний інтерфейс RS-232

12 Ethernet интерфейс

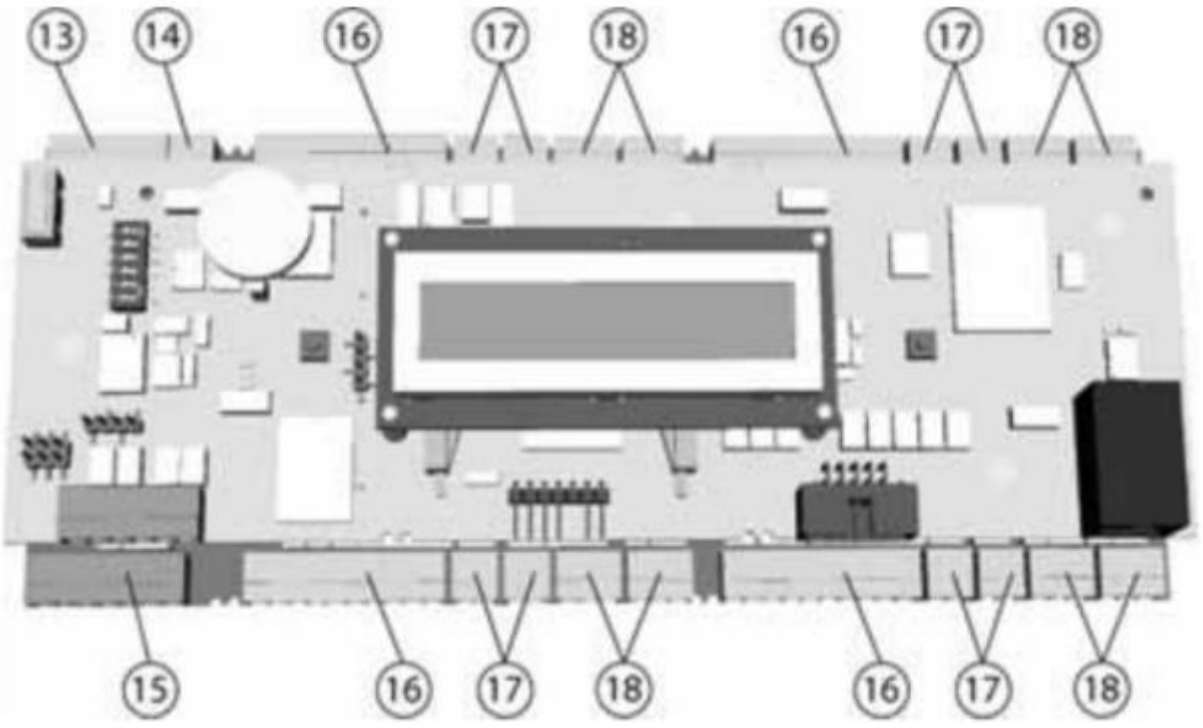


Рисунок 2.11. Нижня частина плати AMC2 4W

13 Шина модуля розширення RS-485

14 Зовнішній контакт датчика розтину

15 Роз'єм джерела живлення

16 Wiegand інтерфейси для до 4 зчитувачів карт

| | |
|---|---|
| 17 | Роз'єми восьми аналогових входів |
| 18 | Рознімання восьми релейних виходів |

На кожних дверях встановлена пара зчитувачів Lectus 3000, зовнішній вигляд зображена на рисунку 2.12.


Рисунок 2.12 Зчитувач карт

Зчитувачі LECTUS Duo можна підключити до допомогою інтерфейсу Wiegand або послідовного інтерфейсу RS485. DIP-перемикачі відповідають за налаштування.

## 2.2. Системи відеоспостереження

Для запису зображення обличчя обрано камеру типу пін хол, яка не зможе створити дуже якісне зображення, але має основну перевагу у тому, що є суттєво дешевшою завдяки відсутності лінзового об’єктиву. Крім того камера стає дуже малопомітною, бо розмір отвору малий, його можна замаскувати масивом глухих поглиблень на поверхні біля основного отвору, імітуючи декор. Виявити таку камеру ще буває складно завдяки відсутності відблискуючих елементів (лінз).

Але низькі можливості камери передавати дрібні деталі зображення вимагають досить крупного кадрування обличчя для кращого розпізнавання. В реальних умовах люди мають різний зріст, можуть зупинитись на різній відстані від камери і крупності облич для фіксованої камери можуть мати суттєві розбіжності. Автоматичне вирівнювання розміру зображення обличчя

в межах розміру матриці є актуальною задачею. Цифровий zoom тут не є прийнятним, бо ще більше погіршить якість зображення. Можливим рішенням може бути зміна кута огляду камери, це можна досягнути зміною відстані матриці від передньої пластини з отвором.

Коли людина стає перед камерою, система визначає обличчя на зображенні і вимірює його розмір в кадрі. Якщо розмір менший необхідного значення, подається напруга на двигун, і механізм віддаляє площину матриці від площини пластини з отвором, зменшуючи кут огляду камери і цим самим збільшуючи розмір зображення обличчя на матриці. Якщо ж камеру затуляє якийсь предмет, або людина стає поза межами оптимальної зони і лише частина обличчя попадає на зображення, система дає сигнал на наближення матриці до отвору, кут огляду розширюється для отримання повного зображення обличчя необхідної крупності.

Сучасні алгоритми програмного забезпечення обробки зображень виявляють очі і обличчя і це дає можливість реалізувати роботу представленої системи. Ця система відповідає концепції автоматизації керування композицією кадра [16 ], яку висловив у 2015 році український експерт з відео та фототехніки Нечай С. О.

Розрахунок пінхол камери

Розроблена камера повинна бути встановлена біля зчитувачів proximity-зчитувачів карт для додатковаого контролю працівників які проходять крізь двері.

Для початку потрібно обрати матрицю. Матриці поділяються на 2 типи CCD та CMOS,

До переваг матриці CCD відноситься:

1. Низкий рівень шумів.

2. Високий коефіцієнт заповнення пікселів (около 100%).

3. Висока ефективність (відношення числа зареєстрованих фотонов до їх загального числу, пов’язаного з світлочутливою областю матриці, для CCD — 95%).

4. Високий динамічний діапазон (чутливість).

До недоліків CCD матриці відносяться:

1. Складный принцип зчитування сигналу, та технологія виготовлення.

2. Високий рівень енергоспоживання (до 2-5Вт).

3. Дороже в виготовленні.

Переваги CMOS матриць:

1. Висока швидкодія (до 500 кадрів/с).

2. Низьке енергоспоживання (майже 100 разів проти CCD).

3. Дешевше та простіше у виробництві.

4. Перспективність технології( на тому ж кристалі в принципі нічого не варто реалізувати всі необхідні додаткові схеми: аналого-цифрові перетворювачі, процесор, пам'ять, отримавши таким чином закінчену цифрову камеру на одному кристалі. Створенням такого пристрою, до речі, з 2002 року займаються разом Samsung Electronics та Mitsubishi Electric).

До недоліків CMOS матриць належать

1. Низький коефіцієнт заповнення пікселів, що знижує чутливість (ефективна поверхня піксела ~75%, інше займають транзистори).

2. Високий рівень шуму (він обумовлений так званими темповими струмами - навіть у відсутність освітлення через фотодіод тече досить значний струм) боротьба з яким ускладнює та подорожчає технологію.

3. Невисокий динамічний діапазон.

Для своєї камери я обрав CMOS матрицю.

CMOS технологія передбачає розміщення електронних компонентів (конденсаторів, транзисторів) безпосередньо в кожному пікселі світлочутливої матриці.

Типорозмір (або тобто формат) матриці зазвичай вимірюють по діагоналі в дюймах і вказують у вигляді дробу, наприклад 1/4", 1/3", 2/3", 1/2 дюйма та ін.

Перше правило вибору кращої матриці досить просте: при однаковій кількості пікселів (роздільна здатність), чим більше фізичні розміри сенсора – тим краще. У більшої матриці більше пікселі, а значить, вона вловлює більше світла. Пікселі більшої матриці розташовані менш тісно, а значить менший вплив взаємних перешкод і нижчий рівень паразитних шумів, що впливає на

якість одержуваного зображення. Нарешті, більша матриця дозволяє отримати великі кути огляду при використанні об'єктива з однією фокусною відстанню.

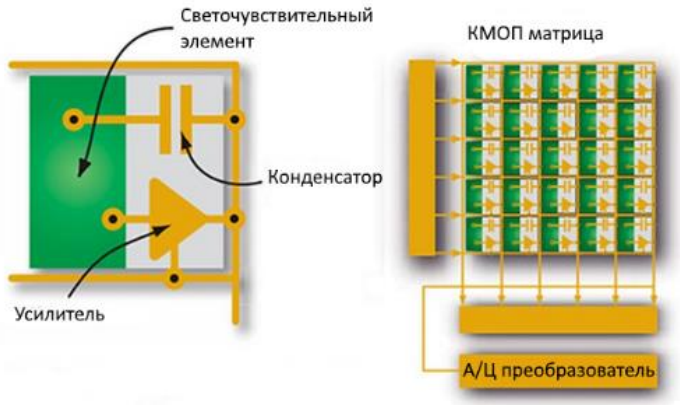


Рисунок 2.13. Будова CMOS матриці.

Виробники вигадали ряд технічних рішень, щоб поліпшити чутливість CMOS матриць та знизити втрати світла в процесі фіксації зображення. Для цього в основному використовується один принцип: винести світлочутливий елемент якомога ближче до мікролінзи матриці, що збирає світло.

Потім прогресивні виробники перейшли на використання матриць із зворотним засвіченням, що дозволяє не тільки скоротити шлях світла крізь матрицю, але й зробити корисну площу світлочутливого шару більше, розмістивши його над іншими електронними елементами в осередку.

Технологія зворотного засвічення дає камері максимальну чутливість. Звідси висновок – «за інших рівних умов» краще придбати камеру використовує матрицю зі зворотним засвіченням, ніж без такої. Конструкцію матриці з CMOS сенором зображено на рисунку 2.14.

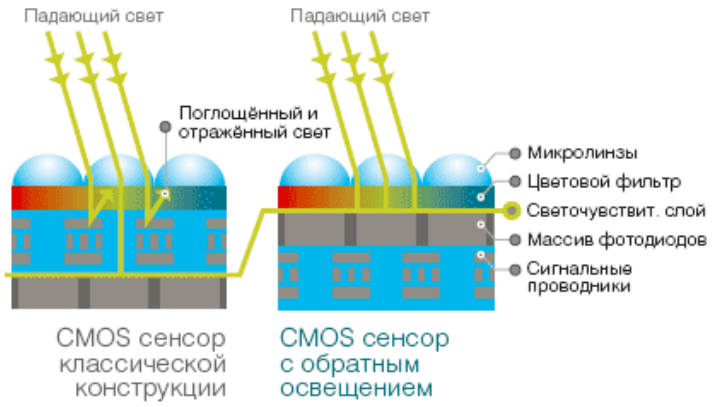


Рисунок 2.14. Конструкція CMOS сенсора.

Для даного приладу обрано матрицю з розмірами 6.3 х 4.7 мм .

Далі проведемо розрахунок розміру отвору.

Розмір отвору розраховується за формулою

$$D = c * \sqrt{f * \lambda} \qquad (1)\ [15]$$

де

D - оптимальний діаметр для отвору.

c – постійна, є коефіцієнтом зі значенням 1.9.

f - фокусна відстань (відстань між точковим отвором та плівкою/датчиком).

λ - довжина хвилі світла, прийнято вважати за λ = 0.00055 мм.

Для розрахунку фокусної відстані скористаємося залежностями трикутників.

Розрахуємо для 2 випадків, 0,5м для випадку коли людина прикладає картку до зчитувача.

2м для випадку коли людина підходить до двері для можливості початкової ідентифікації.

Середньостатистична ширина голови людини складає 25 см, для запобіганню помилок розташування в даному випадку беремо 50 см.

Ширина матриці складає 6.3 мм.

З залежності трикутників відомо що два трикутника що спираються на 2 спільні прямі мають однакові кути. Розглянемо два граничних випадка, коли людина знаходиться біля камери = 500мм та на відстані 2х метрів = 2000мм

Перший випадок

Катет A1 = 500мм – відстань від отвору камери пінхола до лиця.
Катет B1 = 250мм – половина обраної вистоти лиця.

За відношеннями в прямокутному трикутнику знаходимо кут b що є половиною куту обзору.

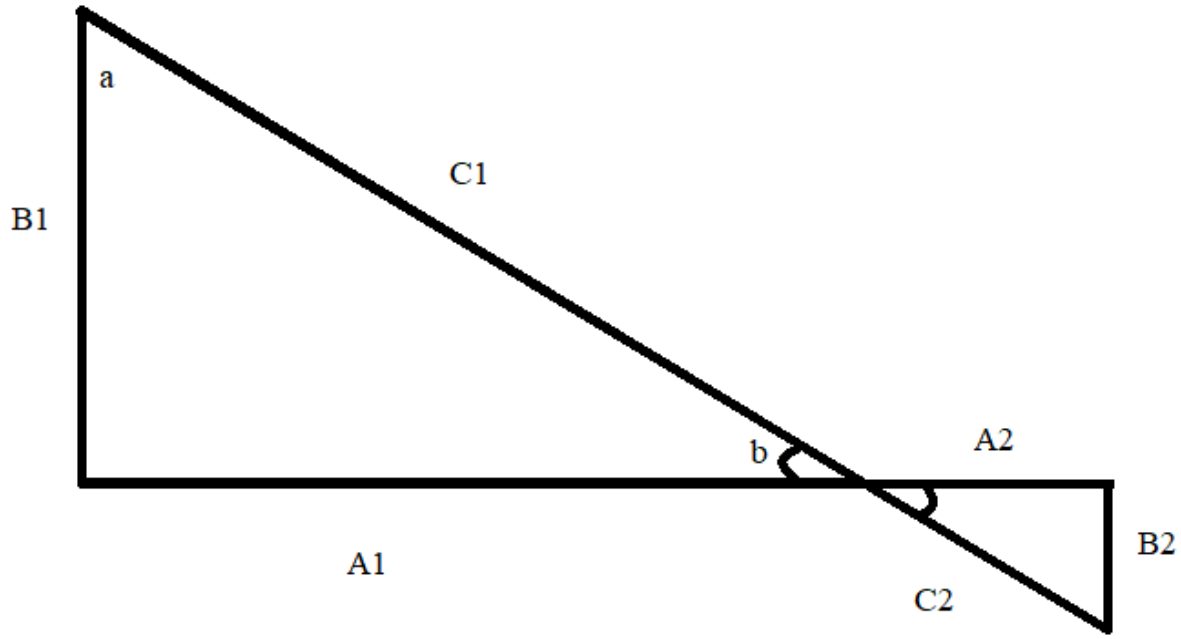


Рисунок 2.15 Залежність трикутників

$$Cosb=A1/C1=A1/(A1^2+B1^2)^{-1/2} \quad (2),$$

Cosb=0.894 мм.

З таблиці косинусів беремо значення кута.

b=26° кут обзору = 2b= 52°.

A2 також знаходимо з залежності прямокутних трикутників.

A2 відноситься до B2 як A1 до B1

Тоді A2 = B2*A1/B1

Максимальну фокусну відстань знаходимо за тим самим принципом.

Другий випадок.

Катет A1 = 2000мм – відстань від отвору камери пінхола до лиця.

Катет B1 = 500мм – для другого випадку зону фіксації лиця розширимо до метру через можливу неточність позиціонування.

$Cosb=2000/(4000000+ 250000)^{-1/2}= 0.9701.$

$b=14^0$, повний кут обзору = $28^0$.

Розрахуємо A2 для другого випадку.

A2 = B2*A1/B1

A2 = 3,15*2000/500 = 12,6мм.

Замінемо кути в першому випадку на 90$^{o}$ та 60$^{o}$ в другому.

Тоді фокусна відстань A2 становитеме:

Для першого випадку 3.15 через те що половина кута обзору дорівнює 45$^{o}$, тоді це стає рівнобедреним трикутником та A2=B2.

Для другого випадку.

A2=tan b*B2.

A2=3.15/tan 30$^{o}$=3.15 /(3$^{-1/2}$/3) =5.455 мм.

Повернемося до розрахунку оптимального розміру отвору (1).

D Для першого випадку.

D = 1.9*(3.15*0.00055)$^{-1/2}$= 0.079 мм.

Діафрагма розраховується за відношенням f /D (3).

Для першого випадку = 3.15/0.079=39.87мм. оптимальною діафрагмою є 32

Розрахуємо оптимальний розмір для другого випадку (1).

D Для другого випадку.

D = 1.9*(5.45*0.00055)$^{-1/2}$= 0.104мм.

Діафрагма розраховується за відношенням f /D (3).

Для другого випадку = 5.455 /0.104= 52.45оптимальною діафрагмою є 32.Для обох випадків час витримки складає 1/25 секунди.

З таблиці еквівалентних пар бачимо що при витримці 1/25при розмірі діафрагми 32 треба обрати вищій показник ISO. Для цього випадку обираємо значення 6400.

| Выдержка, сек | Диафрагма, f | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1,0 | 1,4 | 2,0 | 2,8 | 4,0 | 5,6 | 8,0 | 11 | 16 | 22 | 32 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1/2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1/4 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1/8 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 1/15 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 1/30 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1/60 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1/125 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 1/250 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 1/500 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 1/1000 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Рисунок 2.16. Таблиця еквівалентних пар.

## 2.4. Периметральний датчик

Для лазерного випромінювача лазерний діод ( будову зображено на рисунку 2.17.), (зовнішній вигляд зображено на рисунку 2.18 ) вбудовують в корпус (зображено на рисунку ) з фокусуючою лінзою та металевою конусною призмою зарахунок якої відбувається відбиття світла та розповсюдження його. Лазерний модуль зображено на рисунку 2.19.[12][13]

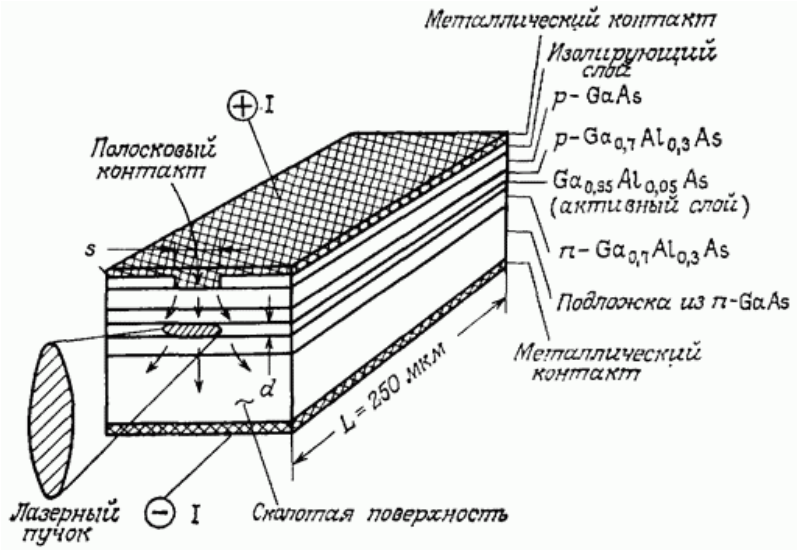


Рисунок 2.17. Будова лазерного діоду( зі збудженням за рахунок струму внапівпроводниках).

Рисунок 2.18 Зовнішній вигляд лазерного діоду

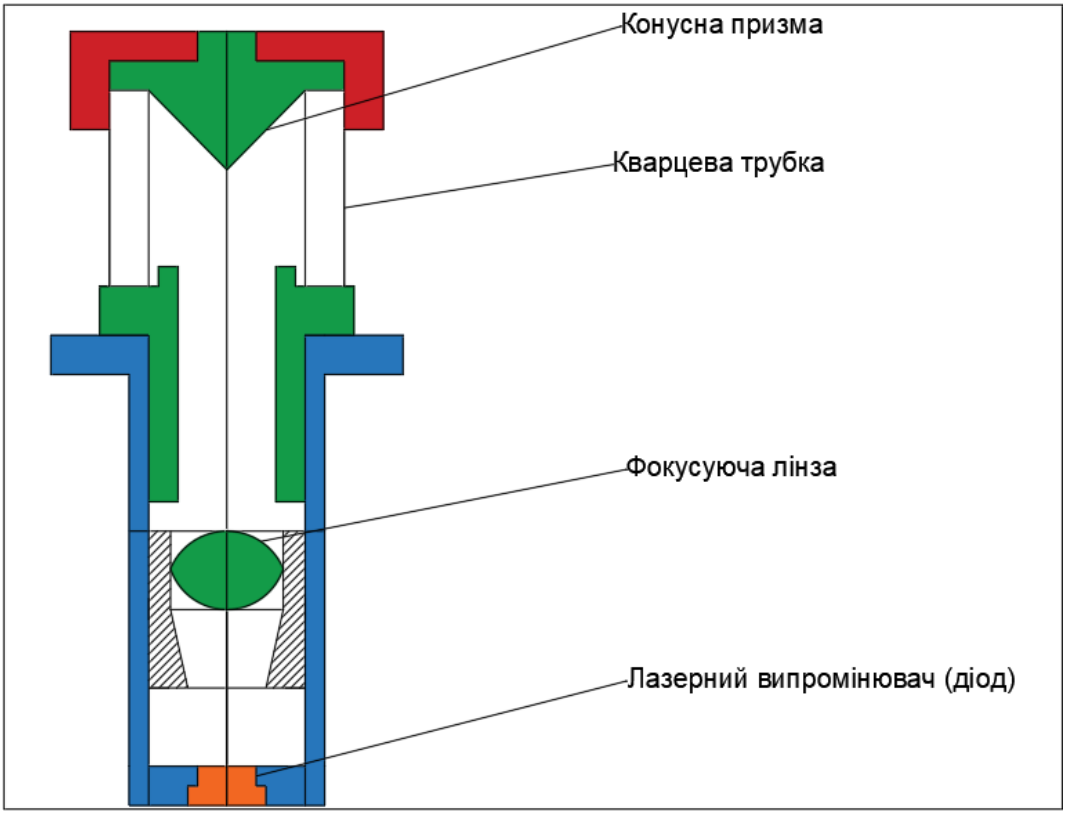


Рисунок 2.19 Будова лазерного модуля.

Розробка лазерного нівеліру потребує знань щодо ефективної фокусноївідстані.Інженерні розрахунки ведуться за наступними формулами:

$$\theta = 2 \cdot \tan^{-1}\left(\frac{x}{2L}\right) \quad (4)$$

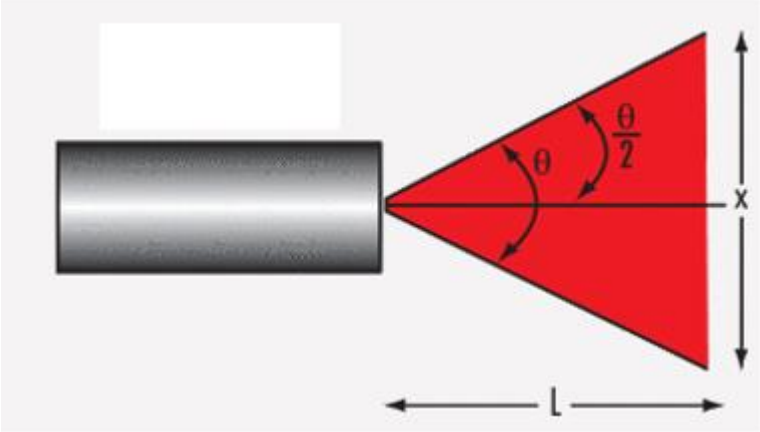


Рисунок 2.20. Наочне зображення параметрів для розрахунку

де θ - віяловий кут пучка, x – необхідна відстань, L –робочавідстань у сантиметрах. Віяловий кут пучка дозволяє розрахувати довжину лінії на заданій робочій відстані:

$$x = 2 \cdot L \cdot \tan\left(\frac{\theta}{2}\right) \quad (5)$$

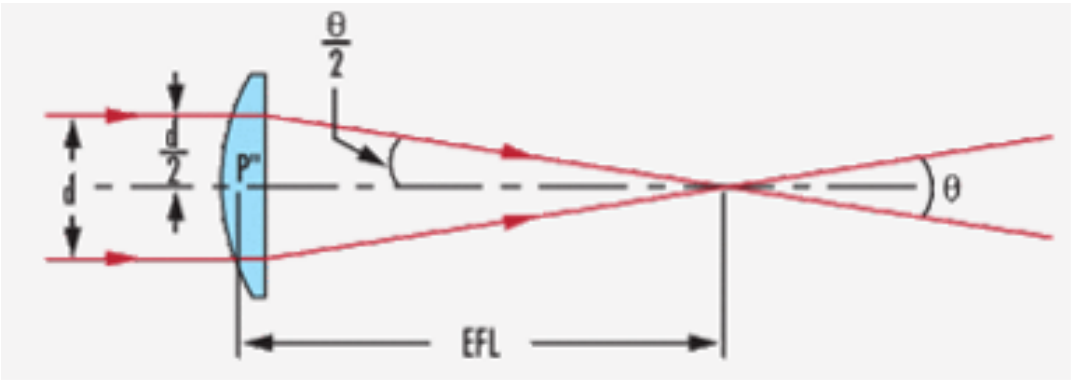


Рисунок 2.21. Знаходження ефективної фокусної відстані

Ефективну фокусну відстаньможна розрахувати знаючи радіус вхідного пучка за наступною формулою:

$$\frac{d}{2} = \mathrm{EFL} \cdot \tan\left(\frac{\theta}{2}\right) \quad (6),$$

де EFL – ефективна фокусна відстань.

Для мого лазерного модулю d = 8 мм, це випливає з середнього діаметру конусноїлінзи при якому розходження променя в обидві боки буде однаковим.

Віяловий кут лазерного діоду (θ) = 15 мрад / 0.85°.3 формули (4) випливає що

$$EFL = \frac{d}{2*\tan\left(\frac{\theta}{2}\right)} = \frac{8}{2*\tan\left(\frac{15}{2}\right)} = 30.38 \text{ мм.}$$

Будова лазерного модуля

Для початку розробки за основу було взято лазерний діод марки Thorlabs, з наступними характеристиками: Довжина хвилі 532 нм; Потужність – 1 мВт; Робочій ток - 220 мА; Дивергенція променя – 15 мрад / 0.85°; Робоча напруга – 2 В. Робоча температура - від -10 °С до 50 °С Зовнішній вигляд якого зображено на рисунку . Розміри зображено на рисунку 2.22.

Рисунок 2.22. Лазерний модуль DJ532

Лазерний діод вбудовано в випромінюючий модуль з наступними розмірами:Довжина – 70 мм;

Товщина стінок – 2мм;

Конусна лінза - 16 мм;

Скло: товщина – 3мм, довжина – 20 мм.

Лазерний модуль з діодом зображено на рисунку 2.23

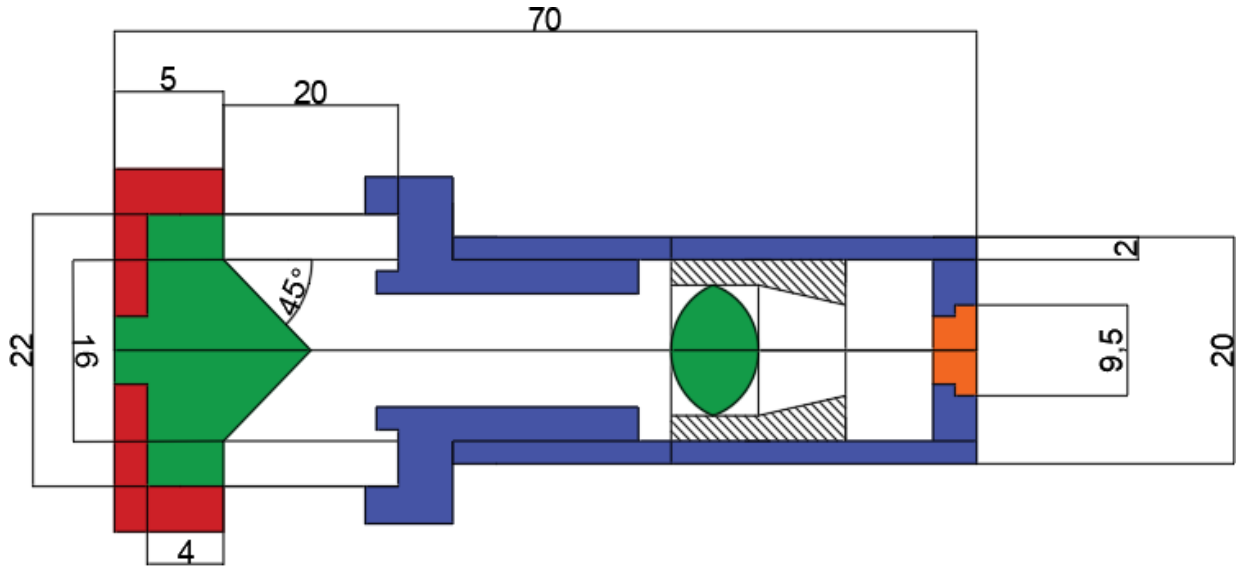


Рисунок 2.23 Лазерний модуль

Проведемо розрахунок відстані на якій фотоелемент може сприйняти світловий сигнал лазеру. Визначення фізичної (параметричної) взаємозамінності.

Для сприймання променю обираємо WO-TPMW1 HIGHLY.

При роботі периметрального датчику важливим фактором є відстань на якій фотоелемент може сприйняти промінь.

Потужність діоду W=1 мВт, сконцентровано в середині кута

$\Omega=Pi*a^2$ [13]

На відстані R від випромінювача (діода) потужність випромінення якаприпадає на одиницю площини поверхні = $W/ \Omega* R^2$. Потужність світла яке потрапляє на фотоелемент на відстані R дорівнює $WS/( \Omega* R^2)$, де S – площа фотоелементу, $S=0,5$ см$^2$.Якщо потужність сприйняття фотоелементом (w) перевищує потужність випромінення тоді фотоелемент може сприйняти промінь. w для фотоелементу становить $w=10^{-13}$ [12][13][14]

$a = \lambda/D$[14]

a – кут дивергенції

λ- довжина хвилі лазерного діоду. Для мого випадку 532нм

D-діаметр початкового пучка

a=0.85.

$w=(W^* S)/Pi^*R^2$, звідси випливає що відстань

$R=((W^* S)/(Pi^*w))^{1/2}$[15]

Для оцінки відстані на якій буде сприйнято відбите світло використана наступнаформула

$R=((W^* S^*Sвідб)/(w^*Pi^* \Omega^* \Omega_1))^{1/4}$(7), де

Sвідб-площа відбиваючої поверхні=0,2м$^2$

$\Omega_1$ - 1/400 – додатковий множник який описує фокусировку відбитого променя

$R=((0.01^*0.5^*0.2)/(10^{-13}*3.14*(0.85)^2*3.14*1/400))^{1/4}$=140 м

Похибка відстані може бути викликана відхиленням початкових параметрів.

S=0,5 ± 0.05 см$^2$ . W = 1 ± 0.03 мВт

a=0.85 ± 0.01

Значення похибок взяті з технічних параметрів лазерного діоду.

Так як зміна параметрів випадкова в межах допустимих норм то

$R_{пох}=(((dr/dS)/\sigma^*K)^2+((dr/dW)/\sigma^*K))^2+((dr/da)/\sigma^*K)^2)^{1/2}$

Часткові похідні по змінних параметрах представляються як

$dr/dS_o=((W^*S)/( w^*Pi^* ^*\Omega_1))^{1/4}=$

$=((0,01^*0,2)/(10^{13}*3.14*(0.85)^2*3.14*1/400))^{1/4}$=0,831 мм/см$^2$

$dr/dW=(( S^*Sвідб)/(w^*Pi^* \Omega^* \Omega_1))^{1/4}= ((0.5^*0.2)/(10^{-13}*3.14* (0.85)^2 *3.14 *1/400))^{1/4}$ = 27,3 Вт/Квт

$dr/da=((W^* S^*Sвідб)^* (w^*Pi^* Pi^*a^2 * \Omega_1)/(w^*Pi^* Pi^*a^2 * \Omega_1)^2)^{1/4}=$
$=((0.01^*0.5^*0.2)/(10^{- 13}*3.14*(0.85)^2*3.14*1/400)^2)^{1/4}$=0,042°

Припускаючи, що випадкові змінні розподілені по нормальному закону, для якогоК=1, отримаємо похибку відстані на який видно промінь:

$\sigma=((0,831)^2*(0,05)^2*(1)^2+(27,3)^2*(0.03)^2*(1)^2+(0,042)^2*(0.01)^2*(1)^2)^{1/2}$=

=8,1926 см/10 м

Отримана похибка складає 0.08%. [15]

## 2.5 Інтелектуальний SMS-сповіщувач

Сповіщувач побудований на базі LSN-модуля та контроллера Arduino. За допомогою програмного забезпечення ACE є можливість передати сигнали як інформацію LSN модулю передає цифровий сигнал на входи контроллера який в свою чергу передає інформацію на програмне забезпечення написане на мові програмування java. Программа сприймає інформацію від контроллера в числовому вигляді що дозволяє програмному забазпеченню сприйняти інформацію з контроллера. Для даного проекту будуть використані піни з 22, 19, 28, 27, 26. Пін 22 використовується для прийому повідомлення про те чи потрібне сповіщення чи ні (1 та 0 відповідно), пін 19 передає інформацію про тип тривоги – 1-проникнення, 2- пожежа, 3- підвищення рівня загазованості, 4 - підвищення температури. Пін 28 – інформація щодо зони, де відбулась надзвичайна ситуація 1, 2, 3, 4 відповідно. Пін 27 відповідає за список отримувачів 1-усі можливі працівники, 2-департамент безпеки, 3- департамент пожежної охорони, 4 - кліматичниа служба, 5 – усі члени команди, які займають керуючі посади, 6- відповідає за 2 та третій списки, 7-2 та 4, 8-2 та 5, 9-3 та 4. 26 пін відповідає за другу частину 1-3 та 5, 2 – 4 та 5, 3 – 2, 3 та 4, 4- 2, 3 та5, 5 – 3,4 та 5. Таким чином в залежності від передаваємої інформації залежить текст сповіщення та отримувачі.

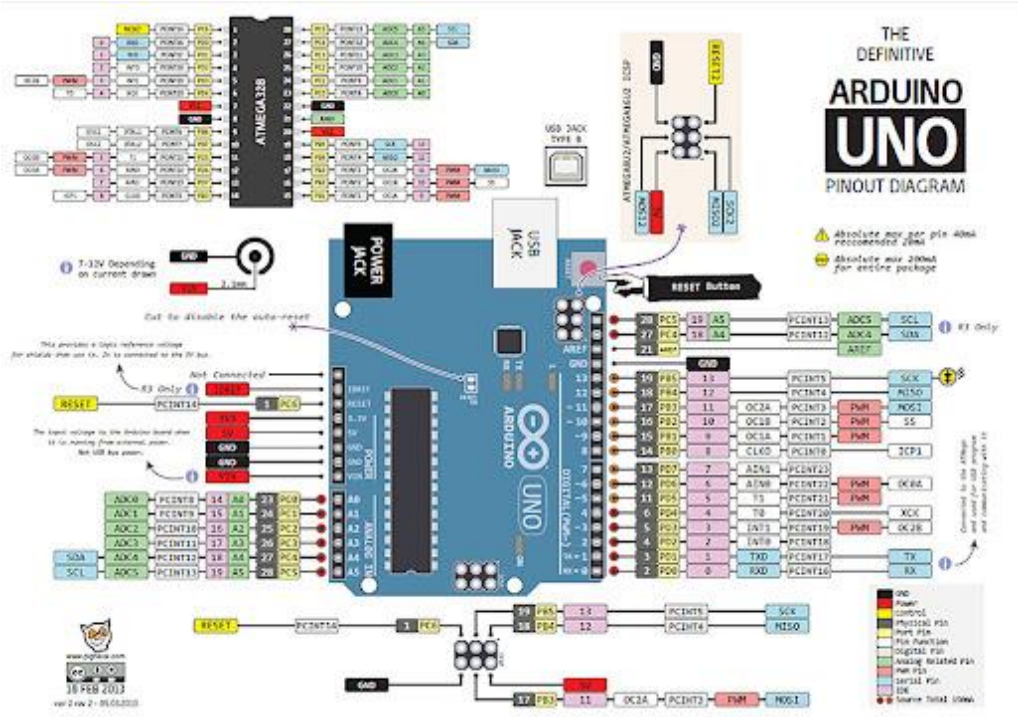


Рисунок 2.24 Схема входів/виходів Arduino Uno

## 2.6. Розрахунок двигуна для переміщення матриці

Даний двигун буде використовуватись для позиціонування матриці відносно отвора в камері пінхолу.

Для даної задачі мною було обрано двигун з потужністю 90 Вт.

Виконавчим механізмом виступає мотор редуктор

Паспортні дані двигуна

| Величина | Значення |
|---|---|
| Номінальна потужність $P_{2n}$, Вт | 90 |
| Номінальна лінійна напруга обмотки статора U1n, В | 12 |
| ККД η | 0.73 |
| Номінальна частота обертання n1, об/хв | 1300 |

| | |
|---|---|
| Коефіцієнт потужності cos ϕ | 0.65 |
| Перевантажувальна здатність λ | 1.3 |
| Число пар полюсів $p_n$ | 2 |
| Номінальне ковзання $S_n$ | 0.053 |
| Момент інерції кг*м$^2$ | 0.00038 |
| Критичне ковзання $S_k$ | 0.363 |
| Кратність пускового струму $k_i$ | 4 |
| Кратність пускового моменту $k_n$ | 2.2 |
| Номінальна частота напруги статора f, Гц | 50 |
| Параметри редуктора | |
| Передаюче відношення $i_p$ | 100 |

Розрахуємо частоту напруги статора:

$\omega_{0n} = 2 * 3.14 * f = 2 * 3.14 * 50 = 314.16$ (рад/с).(1)

Синхрона швидкість обертання двигуна:

$\omega_{xx} = pi * n_0 / 30$ (3.2),

де $n_0 = 60 * f / p_n = 60 * 50 / 2 = 1500$(об/хв), (2)

Тоді $\omega_{xx} = 3.14*1500/30= 157$ (рад/с).

Перейдемо до розрахунку кутової швидкості обертання:

$\omega_n = \omega_{xx}*(1- S_n) = 157*(1-0.053) = 148.679$ (рад/с). (3)

Розрахунок номінального моменту двигуна:

$M_n= P_{2n}/ \omega_n= 90 / 148.679 = 0.6053$ (Нм). (4)

Розрахуємо критичний момент двигуна за переважувальною здатністю λ:

$M_к = \lambda * M_n = 1.3 * 0.6053 = 0.78689$ (Н*м). (5)

Розрахунок номінального значення діючої напруги проведемо за наступною формулою:

$U_n = U_{1n} / 3^{-1/2} = 12 / 3^{-1/2} = 6.9282$(В). (6)

Тоді номінальний діючий струм статора буде:

$I_n = P_{2n} / ( 3 * U_n * \eta * \cos \phi) = 90 / ( 3 * 12 * 0.73 * 0.65 ) = 5.26$ (А). (7)

Для розрахунку фазової напруги скористаємося формулою (8).

$U_{na} = 2^{-1/2} * U_n = 2^{-1/2} * 12 = 8.48$ (В). (8)

Амплітудне значення струму статора становить:

$I_{na} = 2^{-1/2} * I_n = 2^{-1/2} * 5.26 = 7.43$ (А). (9)

Амплітудне значення потокозчеплення статора в режимі холостого ходу при $R_1 = 0$:

$\Psi_{1xx} = U_{na} / \omega_{0n} = 8.48 / 314.16 = 0.026$ (А). (10)

Перейдемо до розрахунку редуктора.

Знайдемо частоту обертання вихідного валу редуктора, вихідний обертовий момент та максимальний обертовий момент.

Частота обертання вихідного валу:

$n_2 = n_1 / i_p = 1300 / 100 = 13$ (об/хв). (11)

$M_2 = M_n * i_p * \eta_2 = 0.6053 * 100 * 0.95 = 57.5$ (Н*м), (12)

де $\eta_2 = 0.95$ – ККД для двоступінчастого редуктора.

Перейдемо до розрахунку максимального обертового моменту.

$M_{2max} = M_n * i_p = 0.6053 * 100 = 60.53$ (Н*м). (13)

Знайдемо діаметр валу.

$d_в = 1.5 *(N/n)^{-1/2}$, (14)

де N – потужність,

n – частота обертів.

$d_в = 1.5 * ( 0.08 / 13 ) = 0.1176$ (см).

На рисунку 2.25 зображено розміщення складових в пінхол-камери. Зображення що потрапляє до матриці за допомогою шини BDB (Bosch Data Bus) передається на сервер де ПО BVS (Bosch Video System) проводить його аналіз та передає центральній системі наказ шодо приближення чи віддалення матриці від отвору. За допомогою EMIL блоку та перетворювача є можливість подати електроенергію двигуну за рахунок якої буде обертатись вал та призведе до руху черв`ячної передачі, яка в свою чергу прикріплена до задньої стінки пластини на якій закріплена матриця. Такий механізм дає змогу рухати матрицю пінхол-камери що буде змінювати фокусну відстань, а це буде впливати на інші параметри фотоможливостей даного приладу.

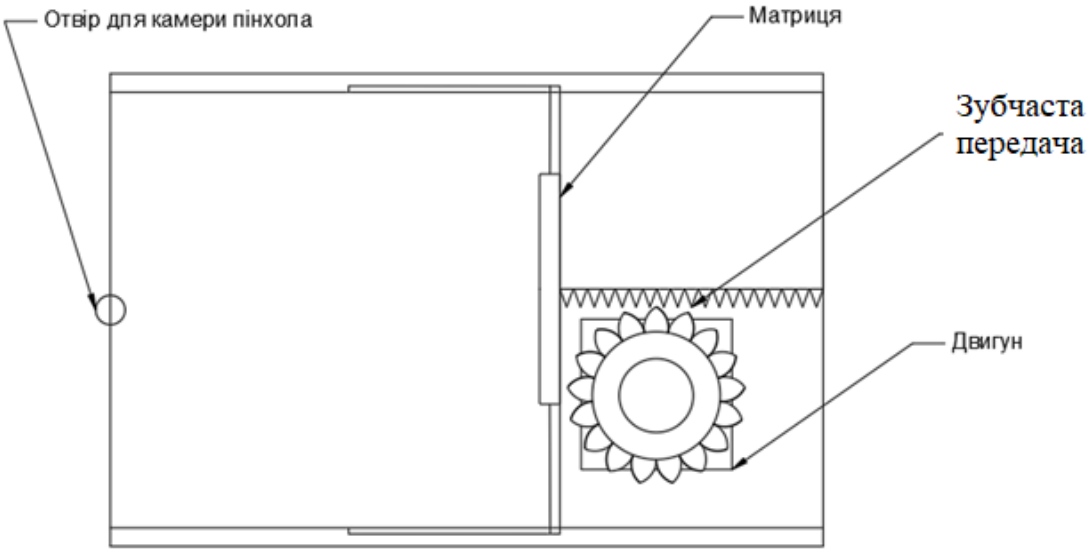


Рисунок 2.25

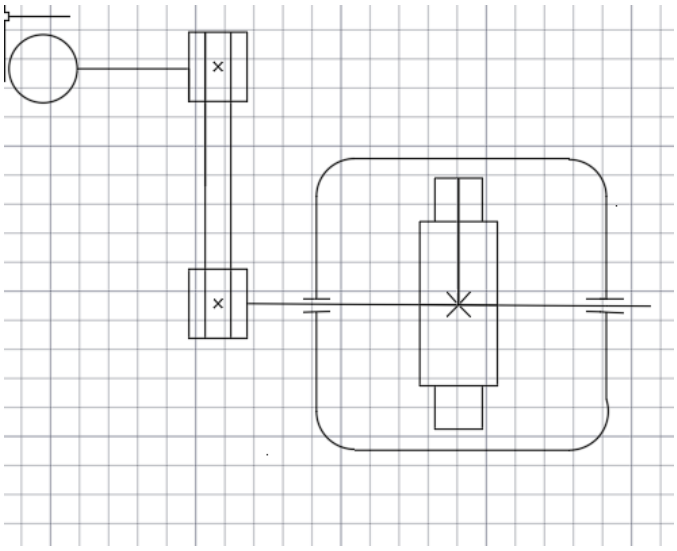

Рисунок 2.26 кінематична схема.

**Висновки до розділу 2.**

В розділі 2 на основі принципів засвоєних в розділі 1 була розроблена система безпеки на основі існуючого програмно-технічного комплексу Bosch Security Systems. Були обрані оптимальні рішення для даного випадку.

В даному розділі усі системи до яких відносятся система запобігання пожежам, система контролю керування доступу, датчик кліматичного контролю та відеоспостереження були об`єднані в загальний комплекс.

Розраховані оптимальні значення діафрагми для створеної пінхол-камери та обраний параметр ISO.

Створено переметральний датчик, напрямлений на запобіганню незаконному проникненню.

Створено концепт смс-сповіщувача. Цей прилад напрямлений на своєчасне сповіщення відповідального за функціонування певної системи своєчасно отримувати інформацію щодо винекнення тривог під час їх знаходження поза зоною контролю безпеки.

## 3. Розробка стартап-проекту

В даному розділу проведено аналіз стартап проекту “Інтелектуальний SMS-сповіщувач тревог”.

Інтелектуальний сповіщувач тривог базується на протоколі SMPP. SMPP – однорангова передача коротких повідомлень. Є відкритим протоколом у телекомунікаційній галузі, який розроблений спеціально для забезпечення гнучкий інтерфейс для обміну SMS-повідомленнями між прикладними SMS-платформами, маршрутизаторами та центрами служби коротких повідомлень.

Загалом, стартапом є будь-який молодий бізнес, і в англомовних країнах таке слово використовується вже давно. Однак у XXI столітті цей термін набув айтішного відтінку — почали в масовому порядку з'являтися IT-стартапи. На даний момент у російськомовних країнах словом «стартап» називають нові інформаційні проекти, створені з розрахунком на швидке їх зростання і високу, внаслідок цього, капіталізацію.

Стартапи покликані вирішувати проблеми та завдання, які згодом стає можливим вирішити завдяки використанню результатів технічного прогресу. Або, як говорив засновник Twitter'a Ісаак “Біз” Стоун, сучасні високотехнологічні проекти мають служити одній меті: спрощувати користувачам будь-які дії у їхньому повсякденному житті.

Рухати технічний прогрес уперед – не завдання стартапера. Справді, коли ми говоримо про стартапа, навряд чи буде згадано нову перспективну компанію, яка розробляє свою революційну архітектуру мікропроцесорів або фільтруючі наноматеріали.

Однак цілком можливо в рамках однієї невеликої команди створити унікальний програмний продукт, який надає його користувачам інноваційні послуги, і який може виявитися різко популярним та затребуваним у найближчому майбутньому. Так само, не критично складно створити й унікальну комбінацію «заліза» разом із програмним комплексом, що забезпечує його роботу.

За останнє десятиріччя стартап як форма малого але ризикованого підприємства набула велике розповсюдження на території всього світу завдяки глобалізації та збільшенню швидкості обміну інформації через поширення інтернету. В інтернеті можна знайти будь-який товар на усі смаки, навіть якщо в країні де знаходиться споживач немає товару-його можна замовити з закордону. Щє одним фактором розповсюдження стартап проектів стали краудфандингові платформии завдяки яким пересічні люди отримали можливість стати спонсорами цікавих їм проектів, на найпопулярнішій платформі Kickstarter є можливість додати певні подарунки пожертви більше певної суми, такі як сувеніри з принтами компанії, прототипні зразки,

можливість першим спробувати продукт та інші, таким чином ідеї які вирішують проблеми споживачів отримали можливість існувати без великих гравців ринку, лише на ентузіазмі винахідників та зацікавленості людей. Великі гравці в свою чергу мають змогу провести моніторинг ринку та на основі отриманих даних зробити висновки щодо ідеї, та як це часто буває викупити стартап та зробити його частиною одного зі своїх продуктів.

Кожен стартап проект повинен привнести до ринку нову або адаптовану до місцевого ринку ідею, яка зацікавить велику кількість потенційних споживачів.

### 3.1 Опис ідеї проекту

Ідея проекту полягає в використанні приладу для сповіщення про наявність тривог персоналу до яких можна віднести членів відділу безпеки, членів протипожежної безпеки та керівництва підприємства під час їх знаходження поза територією підприємства, офісної будівлі чи іншого охоронюємого об`єкту. Прилад отримує інформацію про появу нових тривог яка потрапляє з автоматизованої системи безпеки до складу якої входять система контролю керування доступу до якої входять контролер на вхідних дверях та датчики відчинення дверей, пожежна система до якої входить датчики диму, температурні датчики, датчики контролю клімату, система відеоспостереження до якої також входять датчики руху, програмне забезпечення яке знаходиться на сервері передає сигнал на контролер внутрішньої системи який в свою чергу передає інформацію на зовнішній контролер який оброблює її та створює на основі інформації запит на компанію постачальника смс-трафіку з текстом сповіщення та переліком адресатів, таким чином відповідальні за безпеку певної зони не будуть отримувати сповіщення про наявність тривог на іншій зоні.

Метою данної розробки є допомога керуючому складу персоналу в контролі винекнення небезпеки, своєчасній та адекватній реакції на неї, облік виникших небезпек під час відсутності на робочому місці.

Використовуючи морфологічний метод оберемо оптимальну ідею продукту.

Таблиця 5.1. Проміжні рішення продукту.

| Основні параметри | Проміжні рішення | | |
|---|---|---|---|
| | 1-ше | 2-ге | 3-тє |
| Мова програмування | Python | C++ | java |
| Режим роботи | За запитом | Безперервний | Безперервний |

| | | | |
|---|---|---|---|
| Можливість перенавчання | З можливістю перенавчання | Без можливості перенавчання | Інше |
| Кількість зчитуваних даних | Стала | Адаптивна | Інше |
| Версія програми | Скрипт | Повноційна програма | Програма з веб інтерфейсом |
| Датчики | В комплекті | Закуповуються окремо | Прив’язка до датчиків замовника |

Далі сформований в першій частині продукт стартапу спробуйте розвинути на основі прикладу П. П. Суркова.

Таблиця 5.2. Опрацювання питань для удосконалення продукту.

| № з/п | Запитання | Відповідь |
|---|---|---|
| 1. | Частиною яких систем є продукт? | Продукт є частиною інтегрованої системи безпеки. |
| 2. | Чи можна розділити продукт на частини? | Ні, прилад є завершеним продуктом. |
| 3. | Чи можна об’єднати (агрегувати) кілька елементів продукту в один? | Всі елементи продукту працюють для вирішення однієї задачі та вже об`єднані в один продукт. |
| 4. | Яким має бути ідеальний продукт? | Продукт повинен відповідати стандартам якості замовника, при цьому не втручаючись в логіку роботи приладу. |
| 5. | Що відбудеться, якщо вилучити продукт? Чим його можна замінити? | При вилученні продукту системи безпеки втрачають можливість автоматичного інформування персоналу, які знаходяться поза територією виробництва. |

| | | |
|---|---|---|
| 8. | Яким цей продукт був у минулому? | Люди самостійно переглядали та аналізували дані з датчиків. |
| 9. | На розвиток яких функцій було спрямоване удосконалення продукту? | Головним чином на автоматизацію сповіщень. |
| 10. | Які функції залишилися «недорозвиненими»? | Функція автоматизованого керування ще залишилася недорозвиненою. |
| 11. | Як можна натепер розвинути ці функції? | Програма сама викликає відповідні служби, таких як поліція чи пожежна бригада. |

Зміст ідеї, напрямки застосування ідеї потенційні ринки, групи потенційних клієнтів вигоди які може отримати користувач наведено в таблиці 5.3.

Таблиця 5.3. Опис ідеї проекту

| Зміст ідеї | Напрямки застосування | Вигоди для користувача |
|---|---|---|
| Використання сповіщувача для автоматизованого інформування відповідальних співробітників про появу тривог, таких як проникнення чи пожежна тривога | Система безпеки на промисловому центрі або будівлі | Своєчасне інформування відповідальних співробітників які знаходяться за територією охороняємої території на відміну від GSM передатчиків які отримують сигнал в певній області. |
| | Автоматизоване інформування відповідальних осіб | Інформування лише тих осіб які повинні отримати інформацію та не включення в перелік тих, хто не |

| | | |
|---|---|---|
| | | повинен отримати інформацію |

Отже, пропонується новий автоматизований спосіб інформування членів відділу безпеки та інших відповідальних осіб. Цей спосіб виключає потребу інформування кожного члена команди, інформування відбувається одночасно. Таким чином керуючий відділу безпеки отримавши повідомлення може приймати рішення чи потрібно йому втручатись або команда вирішить питання без його втручання.

Далі проводимо аналіз потенційних техніко-економічних переваг ідеї порівняно із пропозиціями конкурентів:

− визначаємо перелік техніко-економічних властивостей та характеристик ідеї;

− визначаємо попереднє коло конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проводимо збір інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів-конкурентів відповідно до визначеного вище переліку;

− проводимо порівняльний аналіз показників: для власної ідеї визначено показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні) (табл. 5.4).

Таблиця 5.4. Визначення сильних, слабких та нейтральних характеристик ідеї проекту

| № | Техніко-економічні характеристики ід еї | (потенційні) товари/концепції конкурентів | | W | N | S |
|---|---|---|---|---|---|---|
| | | SMS сповіщувач | GSM сповіщувач | | | |
| 1 | енергоспоживання | Низьке | Низьке | | + | |
| 2 | Термін служби | Не менше 5 років | Не менше 3 років | | | + |
| 3 | Межі області сповіщення | Усюди де є покриття мобільного оператор | В радіусі близько кілометру | | | + |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | а | | | | |
| 4 | Час сповіщення | 10-15 секунд з появи тривоги | До 2 секунд з появи тривоги | + | | |
| 5 | Необхідність використання попередньої обробки даних | Так | ні | | | + |

Запропонований варіант сповіщення запропонований для сповіщення персоналу поза зоною охорони тому час затримки викликаний обробкою запиту операторі не є значною. GSM-сповіщувачі потребують своєчасну заміну енергоносіїв на відміну від SMS-сповіщувача який підключений до загальної електромережі та приймачі, які завжди підключаються до підзарядки. Тому в якості метода інформування є одним з найкращих виборів, так як мобільні телефони майже завжди знаходяться біля власника.

В межах даного підрозділу проводимо аудит технології, за допомогою якої можна реалізувати ідею створення проекту.

Визначення технологічної здійсненності ідеї проекту передбачає аналіз складових які вказані в таблиці 5.5.

Таблиця 5.5. Технологічна здійсненність ідеї проекту

| № п/п | Ідея проекту | Технології її реалізації | Наявність технологій | Доступність техно-логій |
|---|---|---|---|---|
| 1. | SMS-сповіщувач | Передатчик аналогового сигналу | Наявна | Доступна |
| | | Приймач аналогового сигналу | Наявна | Доступна |
| | | Програмне забезпечення для передачі інформації постачальнику | Ненаявне | Доступна |
| Обрана технологія реалізації ідеї проекту: наявна та доступна на ринку | | | | |

Проаналізувавши таблицю можна зробити висновок, що проект має достатньо умов для перевірки своєї працездатності та реалізації ідеї. Програмне забезпечення повинно повністю відповідати умовам технологічного забезпечення, тому існуючого програмного забезпечення немає. Кожне ПО повинно буде записано під певні умови, через це відсутністю ПО можна знехтувати.

### 3.2 Аналіз ринкових можливостей запуску стартап проекту

Визначимо ринкові можливості, які можна використати під час ринкового впровадження проекту, та ринкові загрози, які можуть перешкодити його реалізації.

Це дозволяє оцінити актуальність нашого проекту.

Спочатку проведемо аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (таблиця 5.6).

Таблиця 5.6. Попередня характеристика потенційного ринку стартап-проекту

| № | Показники стану ринку (найменування) | Характеристика |
|---|---|---|
| 1 | Кількість головних гравців, од | 2 |
| 2 | Загальний обсяг продаж, грн/ум.од | 7000 грн |
| 3 | Динаміка ринку (якісна оцінка) | Зростаюча |
| 4 | Наявність обмежень для входу (вказати характеробмежень) | Відповідность тех.регламенту |
| 5 | Середня норма рентабельності в галузі (або по ринку), % | 60% |

На ринці сповіщувачів не багато основних гравців тому вихід на цей ринок не повинно бути важкою, через велику кількість потенційних місць де можна розмістити даний прилад можна зробити висновок що цей ринок є великим. Динаміка ринку є зростаючею та не повиннен зменшуватись через постійну потребу в модернізації систем безпеку. Рентабельність є великою через те що основну складову ціни складає вартість програмного забезпечення що дає змогу виставляти будь-яку цінову планку. Через відсутність явних технічних обмежень вихід на ринок не повинен бути важким.

Рентабельність — поняття, що характеризує економічну ефективність виробництва, за якої за рахунок грошової виручки від реалізації продукції

(робіт, послуг) повністю відшкодовує витрати на її виробництво й одержується прибуток як головне джерело розширеного відтворення. З даної таблиці можна зробити висновок, що ринок є привабливим для входження за попереднім оцінюванням.

Цільова аудиторія проекту – компанії які використовують системи безпеки на своїх об`єктах та планують додати інформування своїх співробітників про винекнення загроз. Ринок систем безпеки є дуже широким тому динаміка є зростаючим.

Надалі визначаємо потенційні групи клієнтів, їх характеристики, та формуємо орієнтовний перелік вимог до товару для кожної групи (табл. 5.7).

Таблиця 5.7. Характеристика потенційних клієнтів стартап-проекту

| № п/п | Потреба, що формує ринок | Цільова аудиторія (цільові сегменти ринку) | Відмінності у поведінці різних потенційних цільових груп клієнтів | Вимоги споживачів до товару |
|---|---|---|---|---|
| 1 | Сповіщення працівників поза зоною охорони | Системи безпеки | Вартість проекту | Зона сповіщення працівників |
| 2 | Великий період стабільності | Системи безпеки | Вартість проекту. | Збільшений період стабільності |
| 3 | Потреба у формуванні інформативного сповіщення | Власники або керівники компаній | Необхідність у простій взаємодії з програмою або звітом | Зручність подання інформації |

У зв`язку з тим що системи безпеки встановлюються на усих підприємсятвах та дуже часто встановлені в офісних будівлях нове рішення буде сприйнято позитивно на ринці, адже подібних приладів, де можна задати текст та автоматично його обирати не багато. Великий період стабільності дуже важливий для систем безпеки через можливість винекнення надзвичайних ситуацій що потребують своєчасної адекватної реакції на ці ситуації.

Споживачами можуть бути як великі компанії, так і пересічні покупці, для узгодження потрібно провести багато процедур. Це не є єдиною проблемою.

При застосуванні даного рішення існують певні загрози. (таблиця 5.8).

Таблиця 5.8. Фактори загроз

| № п/п | Фактор | Зміст загрози | Можлива реакція компанії |
|---|---|---|---|
| 1. | Попиту | Вдосконалення може виявитися не настільки потрібним. | Перерахунок вартостей для підтвердження ефективності |
| 2. | Економічна | Зростання інфляції | Пошук можливостей для заміни частин приладу на більш дешеві |
| 3. | Конкуренція | Створення приладу з інтегрованим ПО з можливістю створення запитів через SMPP протокол | Збільшення перевірок тагарних відгуків |
| 4. | Науково-технічна | Швидкий розвиток науки | Моніторинг наукових новин та пошук новихшляхів вдосконалення |
| 5. | Втручання | Перехоплення інформації smpp-протоколу зловмисниками | Зміна інформації по підключенню по протоколу |
| 6. | Незаконне використання програмного продукту | Користування програми та поширення прогнозів може принести великі збитки | Необхідно впровадження систем захисту та використання приладу. Підписання договору NDA |

При втіленні даного проекту існують певні ризики, тож потрібно мати певну опору в вигляді перших покупців та отримати їх відклики по вдосконаленню проекту.

Але поряд із колом загроз існують і певні можливості які дають можливість позиціонувати свій товар у порівнянні з конкурентами на більщ високій позиції фактори можливостей приведені далі(таблиця 5.9).

Таблиця 5.9. Фактори можливостей

| № п/п | Фактор | Зміст можливості | Можлива реакція компанії |
|---|---|---|---|
| 1. | Конкуренція | Є аналоги з меншим радіусом дії або менш безпечні | Збільшення обсягів інтеграції / покращення елементів ПО для збільшення швидккості передачі даних |
| 2. | Економічна | Зменшення податків в сфері діяльності | Зниження собівартості |
| 3. | Безпеки | Інтегрція в систему безпеки без втручання в роботу самої системи через фактори безпеки | Викликання довіри потенційних клієнтів через те що може отримати лише аналоговий сигнал, тому неможливо отримати дані з системи непередбачені користувачем |
| 4. | Попиту | Підвищення потреби в інформуванні співробітників | Попит |
| 5. | Збуту | Зменшення кола рішень до однієї компанії | Закріплення за собою лідерства у галузі |

Деякі загрози можуть слугувати факторами розвитку нових можливостей проекту, що спонукає до використання нових ресурсі або винаходу додаткових функцій приладу. Фактор безпеки підвищує попит на продукт.

Конкуренція є як фактором загрози так і дає можливість продемонструвати переваги над конкурентними рішеннями.

Далі проведемо ступеневий аналіз конкуренції на ринку

Таблиця 5.10. Ступеневий аналіз конкуренції на ринку

| Особливості конкурентного середовища | В чому проявляється дана характеристика | Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною) |
|---|---|---|
| Тип конкуренції: олігополія | Невелика кількість фірм на ринку | Підтримка високої якості обслуговування |
| За рівнем конкурентної боротьби: національний | Багато систем використовують прототипи для сповіщення в невеликій зоні | Ведучи конкуренцію на національному рівні, компанії необхідно прикласти належні зусилля для охоплення всього національного ринку |
| За галузевою ознакою: внутрішньогалузева | Стосується галузі безпеки та інформування | Необхідно зосередити зусилля на пошуку конкурентних переваг, які дозволять компанії займати стійкі конкурентні позиції на даному ринку |
| Конкуренція за видами товарів: товарно-родова | Між іншими | Реклама напрямлена на цільову аудиторію |
| За характером конкурентних переваг: цінова | Споживач звертає увагуна те, скільки коштуватиме інтеграція нашого проекту у його продукт | Зменшити ціни за рахунок пошуку більш дешевих складових |
| За інтенсивністю:продуктова | Продукт бренду рекламує сам себе та підвищує впізнаваємість бренду | Набір усіх необхідних документів та даних для легкої та вдалої інтеграції |

Аналіз підтверджує що проект через свою специфіку потребує зусиль для того щоб війти та зафіксуватися на ринку та мати можливість запропонувати нове рішення потенційним клієнтам. Клієнти звикли до класичного способу сповіщення клієнтів, для нової моделі буде складно завойувати довіру клієнтів, вартість стане одним з вагомим фактором для прийняття рішення.

Після аналізу конкуренції проведемо більш детальний аналіз умов конкуренції в галузі.

Таблиця 5.11. Аналіз конкуренції в галузі за М. Портером

| Складові аналізу | Прямі конкуренти в галузі | Потенці- йні конкурен-ти | Постачальники | Клієнти | Товари- замін-ники |
|---|---|---|---|---|---|
| | GSM-сповіщувач | Інші фірми з схожими видами сповіщувачів | Елементи у вдосконаленні | Ціноутворення | Замінники з меншою зоною покриття або меншою варіативністю текстів та отримувачів |
| Висновки | Немає високої конкуренції через те, що існуючі решення не дають усіх переваг що дає SMS-сповіщувач | Нові сповіщувачі можуть мати кращій дизайн та інтегрований передатчик через SMPP, без потреби підключення до ПК | - | Потреби клієнті в диктують напрямок руху ринку | На даний час немає товару який міг би повністю замінити запропоновану модель. |

Провівши аналіз конкуренції в галузі за М.Портером можна зробити висновок що товар є конкурентноспроможним в галузі інформування про появу небезпек або спрацювання тривожних датчиків, на національному ринці не існує якісних замін

Після всіх аналізів визначається та обґрунтовуєтеся перелік факторів конкурентоспроможності. Конкурентоспроможність є комплексною категорією, що формується під впливом цілої низки факторів, вплив яких, на думку Н.П. Тарнавської, може підвищувати та зменшувати їх вплив на загальну конкурентноспроможність.

Таблиця 5.12. Обґрунтування факторів конкурентоспроможності

| № п/п | Фактор конкурентоспроможності | Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим) |
|---|---|---|
| 1 | Ціна | Ціна інтеграції впливає на прийняття рішення, але інші переваги сповіщувача переважають недолік більш високої ціни. Також кожен приймач повинен куплятись окремо що в кінці може призвести до перевищення ціни SMS-сповіщувача. |
| 2 | Актуальність | Інформування про виникнення можливих ризиків, втручання на територію об`єкту або винекнення пожежної небезпеки буде завжди актуальною. |
| 3 | Попит | Для підприємств та офісних будівель є важливою можливість сповіщення відповідальних за безпеку працівників які знаходяться поза зоною досягнення класичних сповіщувачів. |
| 4 | Енергоефективність | Продукт є більш егнергоефективним за аналоги за рахунок відсутності потреби в використанні енергоносіїв для GSM приймача, сповіщення приходять на мобільний телефон. |
| 5 | Інноваційність | Іноваційна ідея в галузі безпеки на території України яка може вийти на широкий ринок |

Обгрунтування факторів конкурентноспроможності більшою мірою покладається на іноваційність продукту та спроможність автоматизованого прийняття рішення щодо адресатів та тексту повідомлення. Ціна є фактором яким можна знехтувати так як в залежності від розмірів системи та кількості людей які повинні отримати сповіщення класичні рішення можуть перевищити вартість запропонованого рішення.

Таблиця 5.13 Порівняльний аналіз сильних та слабких сторін DUST_METER»

| № п/п | Фактор конкурентоспроможності | Бали 1-20 | Рейтинг товарів-конкурентів у порівнянні з METER_Company | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | –3 | –2 | –1 | 0 | +1 | +2 | +3 |
| 1 | Наявність патентів | 1 | | | | + | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | Велика кількість постачальників | 18 | | | | | | + | |
| 3 | Висока якість | 17 | | | | | | + | |
| 4 | Зона покриття | 20 | | | | | | | + |
| 5. | Ціна | 11 | | | + | | | | |

Провівши аналіз сильних та слабких сторін можна зазначити що наявність патентів не є обов`язковою через те що більшість функіоналу зав`язана на програмному коді, на який не має прямого патентного захисту. Велика кількість постачальників складових дає змогу швидкої заміни при виникненні дефіцитів на ринці.

З таблиць 5.12 та 5.13 бачимо, що фактори конкурентоспроможності суттєві та мають великий позитивний внесок при впроваджені нового SMS-сповіщувача. Основною перевагою та головним досягненням є зона сповіщення, також великою перевагою є якість продукту.

Таблиця 5.14. SWOT- аналіз стартап-проекту

| | |
|---|---|
| Сильні сторони:<br><br>1. Енергоефективність<br>2. Термін служби<br>3. Зона сповіщення | Слабкі сторони:<br><br>1. Відсутність відомості на ринку<br>2. Великі витрати на рекламу впродовж всього часу рекламної кампанії |
| Можливості:<br><br>1. Збільшення продаж.<br>2. Покращення технічного оснащення та перехід на новий тип сповіщувача без необхідності підключення до ПК<br>3. Зменшення податків в галузі.<br>4. Отримання державних тендерів | Загрози:<br><br>1. Цінова конкуренція в зв`язку з появою подібних моделей від відомих гравців ринку.<br>2. Різка зміна курсу гривні може привести до зменшення попиту, особливо з боку малих фірм. |

SWOT-аналіз підтверджує що незважаючи на користь продукту для виклику довіри потенційних клієнтів та закріплення на ринці потрібно докласти значних зусиль по розповсюдженню інформації щодо переваг на конкурентами, основною загрозою є відсутність попиту через відсутність потреби в інформуванні працівників та неочікувана зміна курса гривні.

На основі SWOT-аналізу розробимо ринкові альтернативи.

Таблиця 5.15. Альтернативи ринкового впровадження стартап-проекту

| № п/п | Альтернатива (орієнтовний комплекс заходів) ринкової поведінки | Ймовірність отримання ресурсів | Строки реалізації |
|---|---|---|---|
| 1 | Стратегія нейтралізації ринкових загроз сильними сторонами стартапу | 60% | 2 місяці |
| 2 | Стратегія компенсації слабких сторін стартапу наявними ринковими можливостями | 75% | 4 місяці |
| 3 | Стратегія виходу з ринку | 80% | 9 місяців |

З зазначених альтернатив обираємо стратегію компенсації слабких сторін стартапу наявними ринковими можливостями. Термін реалізації в 4 місяці є цілком прийнятним для даного стартапу через його відносно не тривалість та можливість провести усі необхідні підготовчі умови перед виходом на ринок

### 3.3 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів, визначення базової стратегії розвитку, визначення базової стратегії конкурентної поведінки,

Таблиця 5.16. Вибір цільових груп потенційних споживачів

| № п/п | Опис профілю цільової групи потенційних клієнтів | Готовність споживачів сприйняти продукт | Орієнтовний попит в межах цільової групи (сегменту) | Інтенсивність конкуренції в сегменті | Простота входу у сегмент |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1. | Промислові компанії | Так | Високий | Низька | Складна |
| 2. | Офісні будівлі | Так | Середній | Низька | Складна |
| 3 | Менеджери відділів закупівлі, продажів | Висока | Залежить від кількості категорій товару | Середня | Середня |
| 4 | Керівники, топ-менеджмент | Низька | Залежіть від кількості контрольованих | Низька | Середня |
| 5 | Власники бізнесу | Середня | Приблизно 5-7 угод на рік | Низька | Висока |
| Які цільові групи обрано:<br>Під час аналізу потенційних груп споживачів було прийнято рішення що компанія буде працювати із промисловими компаніями та з керуючими офісними будівлями. | | | | | |

За результатами аналізу потенційних груп споживачів ми обрали цільові групи промислові компанії та офісні будівлі, яким потрібно своєчасно сповіщувати працівників поза охоронюємою зоною, мій варіант сповіщувача вирішує задачу сповіщення на великі відстані що дозволяє керуючим бути в курсі винекнення усіх неочікуванії подій в будь-якій точці земного шару де є покриття мобільних операторів.

Для роботи в обраному сегменті ринку необхідно сформувати базову стратегію розвитку.

Таблиця 5.17. Визначення базової стратегії розвитку

| № п/п | Обрана альтернатива розвитку проекту | Стратегія охоплення ринку | Ключові конкурентоспроможні позиції відповідно до обраної альтернативи | Базова стратегія розвитку* |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1. | Підсилення сильних сторін стартапу за рахунок ринкових можливостей | Перемовини з клієнтами, які представляють цільові групи потенційних клієнтів | Виокремлення переваг цього приладу у галузях безпеки та сповіщення. | Стратегія акцентування своїх переваг над конкурентними товарами. |

За рахунок того що прямих альтернатив продукту немає потрібно сфокусуватися на сильних сторонах приладу та провести успішні перемови з клієнтами на рахунок поставок даного приладу. За рахунок невиликої собівартості та відкритої можливості для масштабування системи безпеки, так як він поєднується з ПК та передає інформацію на ПО яке передає інформацію мобільним операторам.

Наступним кроком є вибір стратегії конкурентної поведінки за допомогою якої можна (табл. 5.18).

Таблиця 5.18. Визначення базової стратегії конкурентної поведінки

| № п/п | Чи є проект «першопрохідцем» на ринку? | Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів? | Чи буде компанія копіювати основні характеристики товару конкурента, і які? | Стратегія конкурентної поведінки* |
|---|---|---|---|---|
| 1 | Ні | Забирати існуючих в конкурентів | Ні, не буде. | Стратегія підкріплення своїх переваг |

Товар не є першопрохідцем на ринку, але має певні переваги над конкурентами, такі як зона покриття та можливість інетлектуально обирати текст повідомлення для передачі інформації працівникам. Компанія не буде копіювати характеристики конкурентів через те що мій продукт в деяких аспектах випереджає їх.

На основі вимог споживачів з обраного сегменту до постачальника і продукту, а також в залежності від стратегії розвитку та стратегії конкурентної поведінки розробляємо стратегію позиціювання яка визначається у формування ринкової позиції, за яким споживачі мають ідентифікувати проект

Таблиця 5.19. Визначення стратегії позиціонування

| № п/п | Вимоги до товару цільової аудиторії | Базова стратегія розвитку | Ключові конкурентоспроможні позиції власного стартап-проекту | Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових) |
|---|---|---|---|---|
| 1 | Можливість працювати “із коробки” | Відкритість до вирішення питань | Формування лояльних споживачів для підвищення відомості товару на ринці. | Якість. Енергоефективність. Зона покриття. |

Результатом даного підрозділу є система рішень щодо ринкової поведінки компанії, вона визначає в якому напрямі буде працювати компанія на ринку.

## 3.4 Розроблення маркетингової програми стартап-проекту

Під час розроблення маркетингової програми першим кроком є розробка маркетингової концепції товару, який отримає споживач. У таблиці 5.20 підсумовуємо результати аналізу конкурентоспроможності товару.

Таблиця 5.1. Визначення ключових переваг концепції потенційного товару

| № п/п | Потреба | Вигода, яку пропонує товар | Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити) |
|---|---|---|---|
| 1 | Інформування про винекнення надзвичайних ситуацій | Інформування працівників в великій зоні покриття | Збільшена зона сповіщення. |

Маркетингова стратегія повинна базуватися вигоді яку пропонує товар яка в свою чергу розв`язує потребу потенційних покупців. Ключова перевага повинна підкріплювати розв`язок проблеми або мати переваги над тими самими конкурентами що відображено в більшій зоні покриття сповіщеннями.

Таблиця 5.21. Опис трьох рівнів моделі товару

| Рівні товару | Сутність та складові |
|---|---|
| І. Товар за задумом | Інтелектуальний SMS-сповіщувач |

| | | | |
|---|---|---|---|
| II. Товар у реальному виконанні | Властивості/характеристики | М/Нм | Вр/Тх /Тл/Е/Ор |
| | 1. Довговічність.<br>2. Якість. | М – потрібно мати початкові інвестиції для початку виготовлення<br>Нм – По повине бути виконане окремо під кожне замовлення | Ор - прилад може бути воконан однією людиною<br>Е - низька собівартість |
| | Якість: відповідає нормам ДСТУ2499:2017 | | |
| | Пакування: програмне забезпечення записане на переносний накопичувач. Конвертор сигналів упакований в картону коробку. | | |
| III. Товар із підкріпленням | До продажу с 15.10.2021 | | |
| | Після продажу 20.11.2021 | | |

Провівши опис трьох рівнів моделі можна зробити висновок що товар у реальному виконанні відповідає початковій ідеї. Пакування виконане в картоній коробці з пупирачастою плівкою для запобіганню зовнішніх уразнень під час транспортування. До материальних складових відносяться лише об`єм коштів для закупівлі складових.

Наступним кроком є визначення цінових меж, якими необхідно керуватися при встановленні ціни на потенційний товар, це передбачає аналіз цін товарів конкурентів, та доходів споживачів продукту (табл. 5.20).

Таблиця 5.2. Визначення меж встановлення ціни

| № п/п | Рівень цін на товари-замінники | Рівень цін на товари-аналоги | Рівень доходів цільової групи споживачів | Верхня та нижня межі встановлення ціни на товар/послугу |
|---|---|---|---|---|
| 1 | 3000-10000 | 3000-10000 | Близько 200000 | 5000-10000 за продукт, та абонентська плата |

Товари замінники/аналоги мають подібний ціновий діапазон до ціни мого продукту. Так як основними клієнтами є компанії то оцінити рівень доходів компанії дуже складно, але на мій погляд немає сенсу встановлювати прилад

в домашню систему безпеки через те що є більш прості товари аналоги з меншим функіоналом, та без можливості інтелектуально обрати текст повідомлення, але для використання на невеликому об`єкті непотрібно вказувати місце винекнення загрози.

Таблиця 5.23. Формування системи збуту

| № п/п | Специфіка закупівельної поведінки цільових клієнтів | Функції збуту, які має виконувати постачальник товару | Глибина каналу збуту | Оптимальна система збуту |
|---|---|---|---|---|
| 1 | Клієнти проводять закупівлю приладів які можуть бути інтегровані в систему безпеки будівлі чи підприємства | Доставка, налаштування, підтримка. | Канал національної дестрибуції | Пряма |

Для даного товару оптимальною системою збуту є пряма система через те що програмне забезпечення потребує конфігурації під кожен окремий випадок встановлення. Продукт буде продаватись лише на території України через можливі проблеми з`єднання з операторами в інших країнах або можливі заборони деяких складових продукту на рівні національного законодавства. До функцій збуту можна віднести доставку товару, внесення змін до програмного коду через те що різні системи безпеки відрізняються за кількістю зон безпеки та групами отримувачаів сповіщень.

В наступній таблиці проведемо аналіз концепції ринкових комунікацій в якій опишему специфіку поведінки цільових клієнтів, канали комунікації якими користуються потенційні клієнти, користуючись якими можна користуватись для проведення маркетингової кампанії серед потенційних клієнтів. Встановимо завдання рекламного повідомлення та концепцію рекламного звернення.

Таблиця 5.24. Концепція маркетингових комунікацій

| № п/п | Специфіка поведінки цільових клієнтів | Канали комунікацій, якими користують | Ключові позиції, обрані для | Завдання рекламного повідомлення | Концепція рекламного звернення |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | ся цільові клієнти | позиціонування | | |
| 1 | Потенційні клієнти звертають увагу на стислі повідомлення про продукти пов`язані з їх професійною сферою | Інтернет: Месенджери як телеграм, вайбер | Своєчасне інформування персоналу | Донести важливість інформування свого персоналу який знаходиться поза зоною забезпечення безпеки про винекнення можливих загроз | Рекламне звернення повинне бути максимально стислим через те що потенційні клієнти не мають багато зайвого часу |

Проводячи підсумки з таблиці маркетингових комунікацій треба звернути увагу специфіку поведінки цільових клієнтів. Потенційні клієнти не мають достатньо часу через велику зайнятість в своїй сфері, тому оптимальним місцем розміщення рекламного звернення є телеграм, ютуб, вайбер – канали з тематикою систем безпеки або з близьким до систем безпеки наротивом.

**Висновок до розділу 3**

Проводячі підсумки повернемося до ідеї стартапу яка складає використання сповіщувача для автоматизованого інформування відповідальних співробітників про появу тривог, напрямками застосування є використання в автоматизованих системах безпеки. До вигоди для споживачів можна віднести своєчасне інформування відповідальних співробітників які знаходяться за територією охороняємої території на відміну від GSM передатчиків які отримують сигнал в певній області, та Інформування лише тих осіб які повинні отримати інформацію та не включення в перелік тих, хто не повинен отримати інформацію через те що кожен об`єкт який має свою службу безпеки не повинен допускати можливості витоку внутрішньої інформації.

До сильних характеристик можна віднести те що запропонований продукт не гірше за аналоги в енергоефективності, має довший термін служби та ширшу зону сповіщення. Проте до слабкої характеристики можна віднести час сповіщення який складає 10-15 секунд, що значно більший за конкурентів, але перевага в розширеній зоні сповіщення перекриває цей недолік.

Даний продукт є технологічно здійсненним через те що частини конструкції з яких складається прилад є доступними, немає лише програмного забезпечення, але воно повинно бути написано для кожного клієнту тому цим можна знехтувати тому цей продукт є цілком здійсненним.

Провівши аналіз ринкових можливостей запуску стартапу робимо висновок що кількість гравців на ринці є не великим та їх аналоги не мають того самого функціоналу, тому ціна яка є вищою за аналоги є цілком виправданою, а рентабельність дозволить швидко відбити витрати на створення даного приладу.

Характеристика потенційних клієнтів стартапу можна зробити висновок що їх цікавить велика зона сповіщення, вартість, великий період стабільної роботи продукту без необхідності на технічне обслуговування та зручність подання інформації кінцевим отримувачам.

Узагальнюючи проведений аналіз стартап проекту можна зробити висновок, що проект інтелектуальний sms-сповіщувач є реальним, проте має багаторизиків. Вдалося прорахувати його можливості на ринку та загрози. Зараз на нашому ринку немає анонсованих аналогів подібного способу дії,

проте можливо, що згодом вони з’являться, зараз на ринці існують подібні прилади, але вони не мають змогу інтелектуально обирати текст повідомлення в залежності від умов. Проте це може створити ряд перепон, як технічних, бюрократичних, так і фінансових. Тож завдання інтегрувати розроблений продукт в системи наших потенційних клієнтів є реальним, але має мати щось більше, ніж просто прогнози, потрібні чіткі аргументи. Це мають бути сертифікати, статистичні дані, тестування якості системи, можливо навіть встановлення прототипу на базу існуючої системи безпеки для підтвердження того, що прилад є цілком робочім і не суперечитиме існуючим засобам інформування. Адже саме це є основою у вдосконаленні систем безпеки.

Також можна зробити висновок, що значну роль відіграватиме вартість інтеграції. Це те, що у першу чергу впливатиме на рішення керівництва підприємства, адже кінцева вартість його продукту має бути конкурентоспроможною на цьому ринку.

Так як галузь потенційно достатньо широка в Україні, наш проект у теорії матиме попит серед наших виробнків бездротових сенсорних мереж.

Наступний висновок — так як інші виробники ще не анонсували подібних продуктів, у проекту є шанси стати лідером у своїй області.

**Загальні висновки по роботі**

Спочатку були розглянуті існуючі системи безпеки, структурну будову існуючих систем, їх складові. Розглянули конструкцію більшості сповіщувачів. В усіх місцях де може бути встановлена система безпеки вона повинна буде встановлена.

Далі усі системи до яких відносятся система запобігання пожежам, система контролю керування доступу, датчик кліматичного контролю та відеоспостереження були об`єднані в загальний комплекс.

Розраховані оптимальні значення діафрагми для створеної пінхол-камери та обраний параметр ISO.

Створено переметральний датчик, напрямлений на запобіганню незаконному проникненню.

Створено концепт смс-сповіщувача. Цей прилад напрямлений на своєчасне сповіщення відповідального за функціонування певної системи своєчасно отримувати інформацію щодо винекнення тривог під час їх знаходження поза зоною контролю безпеки.

Розроблено стартап проект для запропонованого засобу сповіщення

Проводячі ідея стартапу складає використання сповіщувача для автоматизованого інформування відповідальних співробітників про появу тривог, напрямками застосування є використання в автоматизованих системах безпеки. До вигоди для споживачів можна віднести своєчасне інформування відповідальних співробітників які знаходяться за територією охороняємої території та інформування лише тих осіб які повинні отримати інформацію.

## Перелік використаної літератури


1. В.С.Лаврус. Охранные системы "Наука и Техника", 1996 Серия "Информационное Издание", Випуск 4.
2. Извещатели пожарные: классификация, типы, виды, обозначение. – URL: https://fireman.club/statyi-polzovateley/izveshhateli-pozharnyie-klassifikatsiya-tipyi-vidyi-oboznachenie/
3. Пожарный извещатель. – URL: http://www.techportal.ru/glossary/pojarnyi_izveschatel.html.
4. Електроні картки доступу – URL: https://easy-card.ru/article/527/
5. Геркон – URL: https://electrosam.ru/glavnaja/slabotochnye-seti/oborudovanie/gerkony/
6. Wiegand – URL: https://vkmodule.com.ua/Description/Description4.html
7. RS-485 – URL: https://www.cuidevices.com/blog/rs-485-serial-interface-explained
8. Proximity card reader – URL: https://kintronics.com/how-to-wire-your-door-access-control-system/
9. СКУД – URL: https://studopedia.com.ua/1_30311_sistema-kontrolyu-dostupu.html
10. Bosch security systems – URL: https://www.boschsecurity.com/ru/ru/
11. Створення пінхол-камери – URL: https://www.pinhole.cz/en/pinholecameras/pinhole_01.html
12. ЛАЗЕРНА ТЕХНІКА Ю.М. КЛИМКОВ, М.В. ХОРОШЕВ: http://www.miigaik.ru/upload/iblock/5ee/5ee70d02887034adc11e67cee286392c.pdf
13. РАСЧЕТ ЭЛЕМЕНТОВ ЛАЗЕРНЫХ СИСТЕМ ДЛЯ ИНФОРМАЦИОННЫХ И ТЕХНОЛОГИЧЕСКИХ КОМПЛЕКСОВ В.Ю. Храмов 3. Циліндричні лінзи [Електронна адреса]: https://in-science.ru/library/article_post/cilindricheskie-linzy
14. Рахманов Б.М., Чистов Е.Д. Безпека при експлуатації лазерних установок. М .: Машинобудування. 1981. 113 с.
15. Захаров Є. О. Лазерний рівень https://ela.kpi.ua/bitstream/123456789/35091/1/Zakharov_bakalavr.pdf
16. Нечай С. О. Автоматизація керування композицією кадра при зйомках відеокамерою // Приладобудування: стан і перспективи. Збірник матеріалів XIV Міжнародної науково-практичної конференції, 22-23 квітня 2015 року – К. : ПБФ, КПІ ім. Ігоря Сікорського, 2015. – С. 115-116.

**Додатки**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

**ПРИЛАДОБУДІВНИЙ ФАКУЛЬТЕТ**
**ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ І МАРКЕТИНГУ**

***XVII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених***

# ЕФЕКТИВНІСТЬ ТА АВТОМАТИЗАЦІЯ ІНЖЕНЕРНИХ РІШЕНЬ У ПРИЛАДОБУДУВАННІ

07-08 грудня 2021 р.
м. Київ, Україна

## Збірник праць конференції

КИЇВ 2021

**УДК 681.772.2**

*Є. О. Захаров, студент гр. ПМ-01мп, к.т.н., доц. Нечай С. О.*
КПІ ім. Ігоря Сікорського

# ШЛЯХИ ЗМЕНШЕННЯ ГАБАРИТІВ ФОТОКАМЕР

***Анотація.*** У роботі надана інформація по напрямкам розвитку фототехніки з метою зменшення габаритів камер та об'єктивів, короткий аналіз цих технологій. Окрему увагу приділено безоб'єктивним пристроям.
***Ключові слова:*** фотокамера, об'єктив, пінхол, дифракція.

## ВСТУП

З моменту створення першого фотознімку в 1822 році Жозефом Ньепсом перед винахідниками поставала задача по зменшенню приладів для фіксації зображення. Зменшення досягалось завдяки оптимальній компоновці елементів конструкції, винаходам нових елементів конструкції, які б виконували ту саму функцію, при цьому займаючи менше місця та даючи змогу більш якісної фіксації зображення. Розвиток технологій виробництва фотоматеріалів, зокрема зниження зернистості фотоплівки, дозволило зробити найбільш популярними малоформатні камери (35 мм).

До середини XX століття виготовляли велику кількість моделей фотокамер, які досить компактно складались для транспортування, але при приведенні в робочий стан ставали досить громіздкими. Зменшена жорсткість конструкції таких камер впливала на точність позиціювання об'єктиву та стала причиною того, що цей тип камер залишився лише в історії. В кінці XX - на початку XXI століть складаними були висувні об'єктиви в ряді аматорських фотокамер з незмінною оптикою, але і їх епоха минула, надійність у них виявилась недостатньою.

Зменшення довжини телеоб'єктивів з довгою фокусною відстанню досягали за рахунок компромісних оптичних схем, а також використання криволінійних дзеркал в оптичній схемі (яскравим прикладом є схема об'єктива 500 мм зі світлосилою 8, дуже багато фірм виготовляли об'єктиви такого типу).

В 80-х роках минулого століття почали з`являтись перші цифрові фотоапарати, першою представленою моделлю була DS-1P компанії Fuji, а згодом і електронні відеокамери перетворились у цифровий формат. Спочатку перехід на цифру не дав достатньої для фотографії якості зображення з матрицей 0,1 мегапіксель, але згодом завдяки роботі провідних інженерів виробництв роздільна здатність збільшилось та якість картинки зросла. Таким чином інженери розв`язували одразу 2 задачі по зменшенню розмірів приладу для фотофіксації та збільшенню якості.

В наш час, коли камери встановлені в смартфонах та займають все менше і менше місця, задача по зменшенню знову стає актуальною. Для фіксації об`єкту на камері потрібна певна відстань між лінзами в об`єктиві та об`єктивом та матрицею, ця відстань не може зменшуватись менше певних граничних значень, тому перед винахідниками та інженерами постала задача по знаходженню нових шляхів фіксації зображення [1].

## СПОСІБ РОБОТИ СУЧАСНОГО ФОТОАПАРАТУ

Сучасні цифрові дзеркальні фотоапарати працюють за наступним принципом. Світло проходячи через масив лінз об'єктиву, відбивається від

дзеркал та потрапляє на видошукач, через який людина спостерігає кінцеве зображення. За допомогою пелюсток діафрагми фотограф контролює потік світла, яке потрапляє в середину пристрою. Після натискання кнопки спуску підіймається дзеркало та дає можливість світлу після відкриття затвору попадати на матрицю, яка фіксує зображення. Кожен піксель кольорової матриці має над собою світлофільтр певного кольору. Інформація з електронної світлочутливої матриці перетворюється у цифрову форму, подається у процесор, де вона обробляється за певними алгоритмами. Потім вже готова фотографія передається в пам'ять фотокамери, де вона зберігається і доступна для перегляду користувачеві.

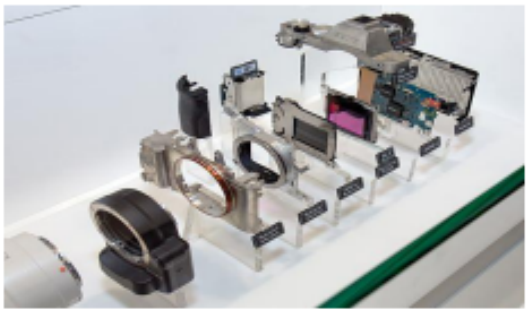

Рисунок 1. SonyAlpha ILCE-7R в розібраному стані

Бездзеркальні цифрові камери вже суттєво компактніші за дзеркальні, бо в них відсутність дзеркала дає можливість зменшити робочий відрізок об'єктивів та від цього і розміри ширококутних об'єктивів. Бездзеркальні цифрові камери можна вважати потомками плівкових далекомірних камер, хоча і при відсутності в них далекомірів і пов'язаних з ними похибок паралаксу. Видошукач бездзеркалки отримує зображення з матриці. На рисунку 1 зображений фотоапарат SonyAlpha ILCE-7R в розібраному стані.

## ВИКОРИСТАННЯ АЛГОРИТМІВ В ОБРОБЦІ ФОТО

В наш час алгоритми цифрової обробки зображення не є новиною. Інженери таких фірм як Sony, Kodak, Canon та виробників мобільних телефонів створюють нові алгоритми обробки зображення, яке потрапляє на матрицю. Таким чином більшість сучасних фото проходить обробку алгоритмами. Ці алгоритми виконують декілька функцій, таких як зменшення шумів, контроль яскравості та ін. Внаслідок використання даних алгоритмів якість кінцевого зображення коригується. Прикладом роботи алгоритмів є технологія HDR, суть якої полягає в тому, що пристрій робить декілька фото, найчастіше три. Перше фото має усереднену експозицію, друге проробляє темні частини кадру, а третє - світлі. Таким чином, поєднавши три зображення, можна отримати багату за напівтонами картинку. Є алгоритми для зменшення ефекту розмиття, коли зйомка проводиться з рук замість штативу. В цьому випадку алгоритми розпізнають більше результатів зйомок, та обирають найкращій, в сучасних моделях смартфонів за це відповідають нейромережі.

## БЕЗОБ`ЄКТИВНІ КАМЕРИ ТА ЇХ АЛГОРИТМИ

Ідея апарату, який дозволяє отримати фото без застосування об`єктиву не нова. Найпростішим приладом є камера обскура, де світло, проходячи крізь тонкий отвір, проецювалося на задню стінку камери в перевернутому вигляді. Відсутність скла в цих камерах дещо зменшує габарити, суттєво зменшує вагу та

ціну камери. Але роздільна здатність зображення в них гірша і пропорційна розмірам камери. Розмір отвору впливає на чіткість зображення, але одночасно і на світловий потік, причому в протилежних залежностях. Кут огляду камери також впливає на розміри камери – чим вужче кут огляду, тим більший розмір між передньою і задньою стінками.

В наш час одразу декілька дослідницьких груп вивчають можливість створення повноцінної безоб`єктивної камери компактних розмірів з якісним зображенням. Традиційні об'єктиви фокусують пучок світла за допомогою рефракції: світло переломлюється при переході через кордон середовищ (повітря-скло) з різними швидкостями світла. Скривлені дзеркала на кшталт тих, що використовують у великих телескопах, формують зображення інакше: з допомогою відображення. Змінити напрямок поширення світла та використовувати його хвильову природу допоможуть два інші фізичні явища: дифракція та інтерференція. При зустрічі двох когерентних хвиль світла вони накладаються одна на одну, виникає результуюча амплітуда хвилі. Якщо максимум однієї хвилі завжди збігається з максимумом іншої, хвилі посилюють одна одну, це називається конструктивною інтерференцією. Якщо максимум однієї хвилі завжди збігається з мінімумом іншої, то хвилі гасять одна одну – це деструктивна інтерференція, в результаті якої світло може взагалі зникнути. Керувати світлом за допомогою дифракції можна, спрямовуючи його на дифракційну решітку – ряд найтонших штрихів (растру) – на гладкій поверхні. Оскільки хвилі з різною довжиною відбиваються у різні боки, виникає колірне фарбування. Через залежність довжин хвиль від растру неможливо створити дифракційну решітку, яка просто замінює лінзи. Оптичне зображення, сформоване гратками, ніколи не виглядатиме так само добре, як зображення з грамотно спроектованого об'єктива. Проте цілком можна створювати прийнятні цифрові зображення за допомогою комбінації дифракційної оптики (що використовує дифракцію) і обробки сигналів, що збігаються (matchedsignalprocessing) (з урахуванням оптики). В одному з класів безоб'єктивних пристроїв для макроскопічної зйомки використовуються мініатюрні дифракційні решітки, ступінчасто розташовані в товщині прозорого матеріалу (скла або силікату), і затримують одну частину падаючого світла щодо іншої частини. Ґратки прикріплені до світлочутливої матриці – на зразок матриці у звичайних цифрових камерах. Падаюче світло проходить через ґратки і досягає масиву, вже особливим чином розкладене на «складові». Виглядає це зовсім не так, як звичайне зображення: якась розмита хмара, незрозуміла для людського ока. Однак ця хмара містить досить візуальної інформації (хоч і незвично розподіленої), щоб відтворити з неї бажане зображення за допомогою обчислювального процесу, який називається згорткою зображення (imageconvolution). На рисунку 2 зображено принцип роботи фотоапарата з дифракційною решіткою.

Алгоритм реконструкції зображення трохи чутливий до візуального шуму, наприклад, випадковим флуктуаціям у кількості фотонів або електричного шуму в ході перетворення сигналу з сенсора в числове уявлення (так звана помилка квантування, quantizationerror). Тому зображення може бути візуально зашумленим. Хоча такої якості достатньо для ряду простих завдань (наприклад, щоб порахувати кількість людей у кадрі).

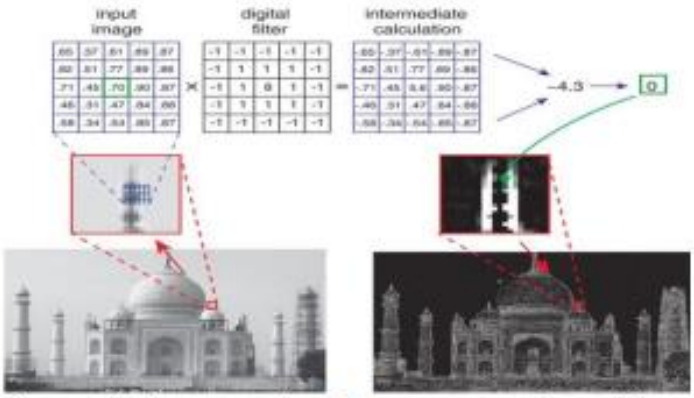


Рисунок 2. Приклад роботи фотоапарата з дифракційною решіткою

Одним з прикладів вдалого застосування даного метода є проект FlatCam, створений дослідниками з Університету Вільяма МаршаРайса. Даний прототип представляє матрицю з накладеною спеціальною маскою з множиною отворів. Маска перетворює камеру на масив пінхол-камер. Інформація з цих камер проходить обробку спеціальним алгоритмом та складається в зображення.

Вартість звичайних камер багато в чому визначається вартістю об'єктивів і наступним складанням, так що виключення об'єктиву зі схеми дозволяє сильно знизити вартість виробу. У конструкції камери, включаючи маску та матрицю, можуть використовуватися лише вже традиційні технології напівпровідникового виробництва, що підвищує масштабованість та знижує ціну. Також камери можуть бути тоншими за 0,5 міліметра і важити менше 0,2 грама, їх можна буде задіяти там, де сьогодні не мають змоги бути застосовані звичні громіздкі пристрої. До того ж, схема FlatCam дозволяє отримати всю необхідну інформацію про сцену, зробивши один кадр, тому можна реалізувати відеозйомку динамічних сцен у реальному часі.

## ВИСНОВОК

Тенденції розвитку алгоритмів обробки інформації, отриманої з фотоприладів, ведуть до збільшення ролі обчислювачів у побудові кінцевого зображення.

Компактні апарати актуальні в системах безпеки, де значною перевагою стануть малий розмір, що дасть значний простір для розташування в місцях, де традиційні камери з об`єктивами привертають багато уваги, та зменшити вартість, що є одним з вагомих факторів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Чи можна зменшити камеру телефона. Режим доступа:www.URL: https://www.androidauthority.com/smartphone-camera-bumps-1195811/ — 10.02.2021 р.

[2] FlatCam: Thin, LenslessCamerasusingCodedApertureandComputationM. SalmnanAsif, AliAyremlou, AswinSankaranarayanan, AshokVeeraraghavan, and Richard Baraniuk. Режим доступа: www.URL: http://imagesci.ece.cmu.edu/files/paper/2017/flatcam_tci17.pdf