Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

(тема)

Виконав:
здобувач 2 року навчання,
групи КТРСм-23-2
Львов А.А.
(прізвище, ініціали)
Спеціальність 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Комп'ютеризовані та робототехнічні системи
(повна назва освітньої програми)

Керівник доц. Сотник С.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри КІТАР _____ Невлюдов І.Ш.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет АКТ
Кафедра КІТАР
Рівень вищої освіти другий (магістерський)
Спеціальність 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(код і повна назва)
Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Комп'ютеризовані та робототехнічні системи
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Львову Андрію Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення комп'ютеризованої системи управління складним електронним замком на базі Arduino з використанням штучного інтелекту

Затверджена наказом по університету від 25.11.2024 №1239 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 16.01.2025 р
3. Вихідні дані до роботи:
3.1 Вимоги до ПК: Операційна система Windows 10 Pro 64-bit,
3.2 ОЗУ 8 ГБ, процесор Intel Core i5-2400 CPU 3.1GHz, Intel HD Graphics
4. Перелік питань, що потрібно опрацювати в роботі
4.1 Вступ;
4.2 Аналіз технічного завдання
4.3 Розроблення структурної схеми системи управління складним електронним замком
4.4 Розробка системи управління електронним замком
4.5 Оцінка надійності та швидкості системи
4.6 Охорона праці

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Слайди у форматі Power Point у кількості 12 слайдів з розширенням .pptx;*

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Приміт-ка
1	Аналіз технічного завдання	11.11 – 17.11.24	вик
2	Аналіз вимог до функціональної структури	18.11 – 19.11.24	вик
3	Аналіз предметної області	20.11 – 21.11.24	вик
4	Розробка системи управління замком	22.11 – 24.11.24	вик
5	Програмна реалізація системи	25.11 – 31.11.24	вик
6	Оцінка надійності та швидкості системи	01.12 – 05.12.24	вик
7	Оформлення пояснювальної записки	06.12 – 07.12.24	вик
8	Подання роботи на рецензію	08.12 – 09.12.24	вик
9	Подання роботи на підпис зав. кафедри	10.12 – 13.12.24	вик
10	Подання атестаційної роботи в ЕК	14.01.25	вик

Дата видачі завдання 11.11.2024

Здобувач _____ Львов А.А.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доц. Сотник С.В.
(підпис) (посада, прізвище, ініціали)

Я, як студент ХНУРЕ, розумію і підтримую політику закладу із академічної доброчесності. Я не надав і не одержував недозволену допомогу під час підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

11.11.2024 Львов А.А.

РЕФЕРАТ

Кваліфікаційна робота містить: 54 с., 1 табл., 21 рис., 2 дод., 19 джерел.

ЕЛЕКТРОННИЙ ЗАМОК, КОМП'ЮТЕРНА МОДЕЛЬ, ARDUINO, ШТУЧНИЙ ІНТЕЛЕКТ, СЕНСОРНА СИСТЕМА, АВТОМАТИЗАЦІЯ.

Об'єкт дослідження є процес автоматизованого управління доступом за допомогою електронного замка.

Предмет дослідження – електронний замок на базі Arduino з використанням штучного інтелекту.

Мета роботи – підвищення безпеки доступу за рахунок розроблення комп'ютеризованої системи управління складним електронним замком на базі Arduino з використанням штучного інтелекту.

В кваліфікаційній роботі розглянуто актуальні питання за темою, запропоновані рішення моделювання роботи електронного замка в середовищі Arduino, а також налаштування сенсорної системи та програмного забезпечення для керування комп'ютерною моделлю замка з використанням штучного інтелекту для забезпечення надійного доступу. Зокрема, розглянуто використання алгоритмів розпізнавання біометричних даних та адаптивного навчання для покращення точності роботи системи.

Результати роботи можна віднести до цілей сталого розвитку 9 та 12: «Промисловість, інновації та інфраструктура», «Відповідальне споживання та виробництво» відповідно.

Отримані результати можуть бути використані на етапах проектування та тестування електронних замків з елементами штучного інтелекту для покращення безпеки доступу в інтелектуальних будівлях, а також в освітньому процесі при проведенні практичних чи лабораторних робіт за спеціальностями, пов'язаними з автоматизацією, робототехнікою та

розробкою інтелектуальних систем.

Результати, що були отримані під час навчання та підготовки кваліфікаційної роботи, висвітлено в статті.

ABSTRACT

The qualification work contains: 54 pages, 1 tables, 21 figures, 2 appendices, 19 sources.

ELECTRONIC LOCK, COMPUTER MODEL, ARDUINO, ARTIFICIAL INTELLIGENCE, SENSOR SYSTEM, AUTOMATION.

The object of the study is the process of automated access control using an electronic lock.

The subject of the study is an electronic lock using hardware and software solutions based on the Arduino platform.

The purpose of the work is to improve access security by developing a computerized control system for a complex electronic lock based on Arduino using artificial intelligence.

Research method – modeling and development of a hardware and software system based on the Arduino platform, development and implementation of artificial intelligence algorithms for analyzing user data and managing access. The qualification work considers current issues on the topic, proposes solutions for modeling the operation of an electronic lock in the Arduino environment, as well as configuring a sensor system and software for controlling a computer model of the lock using artificial intelligence to ensure reliable access. In particular, the use of biometric data recognition algorithms and adaptive learning to improve the accuracy of the system is considered.

The results of the work can be attributed to Sustainable Development Goals 9 and 12: "Industry, Innovation and Infrastructure", "Responsible Consumption and Production", respectively.

The results obtained can be used at the stages of designing and testing electronic locks with artificial intelligence elements to improve access security in

intelligent buildings, as well as in the educational process when conducting practical or laboratory work in specialties related to automation, robotics and the development of intelligent systems.

The results obtained during training and preparation for the qualification work are highlighted in the article.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

БКЗ – блок керування живленням загальний;

МН – машинне навчання;

ГН – глибинне навчання;

ШНМ – штучні нейронні мережі;

AI – штучний інтелект;

DL – глибинне навчання;

GDPR – загальний регламент із захисту даних;

RFID – радіочастотна ідентифікація.

ВСТУП

Метою цієї кваліфікаційної роботи є підвищення безпеки доступу за рахунок розроблення комп’ютеризованої системи управління складним електронним замком на базі Arduino з використанням штучного інтелекту. У роботі буде здійснено проектування та впровадження інтелектуальної системи контролю доступу, яка забезпечить високу безпеку та зручність використання для кінцевого споживача. В результаті цього дослідження буде створено ефективний прототип замка, здатний адаптуватися до змінних умов експлуатації та забезпечити захист від несанкціонованого доступу. Запропонована система не лише надає цю можливість, але й забезпечує зручність контролю завдяки використанню сучасних технологій. В межах цього проекту була створена система, яка, хоча й має аналоги на ринку, вирізняється простотою у використанні та доступною вартістю. Дослідження було зосереджене на впровадженні технології персоналізації і заміни традицій них ключів на відкриття дверей за допомогою радіочастотної ідентифікації (RFID), яка вже широко застосовується в сучасному світі. У сучасну цифрову епоху питання безпеки та контролю доступу стають все більш важливими. Зі збільшенням кількості користувачів та їх потреб сучасні електронні замки стають все більш складними, що ставить перед розробниками таких систем нові виклики, зокрема в контексті забезпечення надійності, безпеки та простоти використання. Одним із напрямків розвитку електронних замків є інтеграція інтелектуальних інструментів, таких як штучний інтелект, машинне навчання та обробка природної мови, які стають передумовою для оптимізації цих систем. Використання таких технологій дозволяє створювати автоматизовані системи контролю доступу, які значно підвищують ефективність роботи, мінімізуючи вплив людського фактору та знижуючи ризик помилок.

Автоматизація процесів управління замками дозволяє збільшити швидкість реагування на запити користувачів і скоротити витрати часу на їх обслуговування. Роботизовані рішення, у свою чергу, сприяють розвитку автономних систем, здатних виконувати складні завдання контролю доступу в реальному часі. Інтеграція цих технологій створює нові, більш адаптивні та гнучкі системи електронних замків, які не лише виконують завдання відкривання та закривання дверей, але також здатні передбачати потреби користувачів на основі аналізу їх поведінки та контексту використання.

Варто також зазначити, що автоматизація сама по собі є ключовим трендом у сучасних технологіях, який може значно покращити управління електронними замками. Використання автоматизованих рішень дозволяє знизити витрати на експлуатацію та технічне обслуговування, одночасно підвищуючи рівень безпеки та продуктивність системи. Автоматизація дозволяє ефективно керувати великими мережами замків, координувати їхню роботу та надавати миттєвий доступ до даних про стан системи, що робить управління замками більш прозорим і контрольованим.

Тому в умовах зростаючих вимог безпеки та автоматизації актуальність аналізу існуючих систем електронного замку стає очевидною. Інтеграція інтелектуальних інструментів, автоматизації та роботизації відкриває нові горизонти для підвищення надійності, швидкості та ефективності електронних замків, одночасно забезпечуючи максимальну зручність користувача.

Мета роботи – підвищення безпеки доступу за рахунок розроблення комп’ютеризованої системи управління складним електронним замком на базі Arduino з використанням штучного інтелекту.

Об’єкт розробки є процес автоматизованого управління доступом за допомогою електронного замка.

Предмет розробки – процес управління електронним замком із використанням апаратно-програмних рішень на базі платформи Arduino та алгоритмів штучного інтелекту.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести аналіз існуючих систем електронних замків;

– провести вибір методу застосування штучного інтелекту в системах безпеки;

– провести аналіз вимог до систем електронних замків з використанням штучного інтелекту;

– провести розробку системи управління замком;

– провести розробку алгоритму системи;

– впровадження AI-модуля для розпізнавання обличчя;

– розробка програми для системи на базі Arduino;

– провести оцінку надійності та швидкості системи;

– оформити кваліфікаційну роботу згідно ДСТУ 3008:2015 [1], а також з методичними вказівками з підготовки й оформлення кваліфікаційної роботи здобувачами другого (магістерського) рівня вищої освіти спеціальності 174 Автоматизація, комп’ютерно-інтегровані технології та робототехніка [2].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз існуючих електронних замків

Електрозамок – це виконавчий елемент системи контролю та управління доступом (СКУД), призначений для запобігання потраплянню сторонніх осіб у приміщення. За своєю конструкцією він схожий на звичайний замок: буває врізним або накладним, може керуватися натискними чи фіксованими ручками, а також відкриватися ключем. Багато електрозамків мають розміри, аналогічні звичайним механічним замкам. Основною відмінністю є додатковий спосіб керування.

Для роботи електричної частини до замка підводять джерело живлення, яке підключається до пристрою керування. Це можуть бути зчитувачі карт, біометричні датчики, кодонабірні клавіатури, брелоки або дистанційні пульти. Відкривання та закриття замка відбувається шляхом подачі або вимкнення електричного струму.

Це створює головну перевагу і причину чому використовуються такі замки – вони дозволяють відчиняти двері дистанційно та без застосування механічного ключа. Принцип роботи електрозамків на (рис. 1.1) [3].

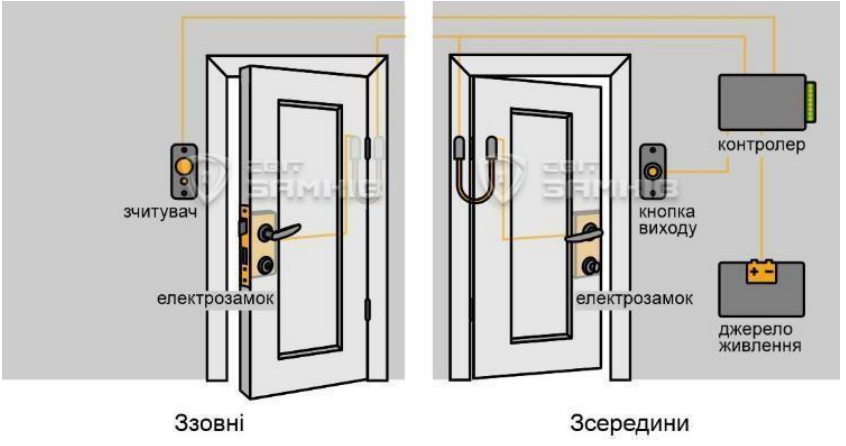

Рисунок 1.1 – Принцип роботи електрозамків

Основне, що потрібно знати про роботу електрозамків в залежності від подачі чи зняття живлення це те, що вони поділяються на "нормально замкнені", "нормально відімкнені" та "універсальні".

Нормально замкнений це означає, що розблокування закритого замка відбувається при подачі електричного сигналу. При його відсутності – замок зачинений.

Нормально відімкнений. За наявності електричного сигналу замок залишається зачиненим, а при припиненні подачі – відкривається.

Універсальний. Такі пристрої мають перемикач, за допомогою якого можна самостійно налаштувати потрібний режим роботи.

При встановленні електронних замків важливі не лише надійність системи, а й якість монтажу. Вона впливає на функціональність, довговічність замка та рівень безпеки. Недотримання технологічних вимог може призвести до збоїв, зниження захисту або передчасного зносу обладнання. У цьому розділі розглянемо ключові аспекти монтажу електрозамків для оптимальної роботи системи контролю доступу та уникнення поширених помилок.

Для початку розглянемо перший варіант схема 1 – найпростіша схема комутації електромеханічного замку, використовуючи яку можна забезпечити дистанційне відкриття дверей рис. 1.2 [3-6]. З особливостей – необхідно зазначити, що для стабільної роботи буде потрібний досить потужний блок живлення. Також зауважимо, що тривале натискання на кнопку (більше 3-5 сек) в більшості випадків призведе до згоряння втяжного реле замка.

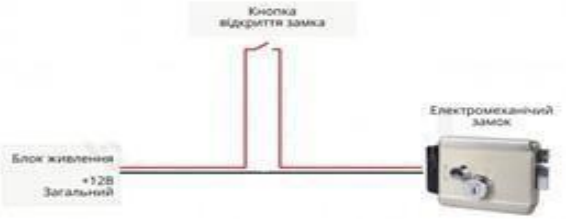

Рисунок 1.2 – Підключення електромеханічного замка за допомогою блоку живлення для дистанційного відкриття дверей

Далі проведемо огляд – схема 2 для електромеханічного замка у більш правильному варіанті, використовуючи блок керування замком (БКЗ) (рис. 1.3) [3-6]. Цей варіант дозволяє використовувати звичайний блок живлення та обмежує тривалість подачі напруги на замок. Блок керування живленням (БКЗ) розміщується у тілі замка або поблизу нього. Недоліками такого монтажу є ризик виходу з ладу БКЗ, що може бути пов'язано з його низькою вартістю та якістю складання, яка залежить від партії постачання.

Рисунок 1.3 – Підключення електромеханічного замка за допомогою блоку живлення та пульта дистанційного відкривання дверей

Третій варіант – схема 3 і тут можна побачити «класичну» (і вже застарілу) схему підключення відеодомофону та електромеханічного замку (рис. 1.4). Такий тип підключення повсюдно використовувався до появи на ринку блоків управління замком (БУЗ), і має ті ж конструктивні недоліки, як і варіант, зображений на схемі (рис. 1.4) [3-6]. Зазначимо, що управління замком у більшості сучасних домофонних систем здійснюється за допомогою панелі виклику.

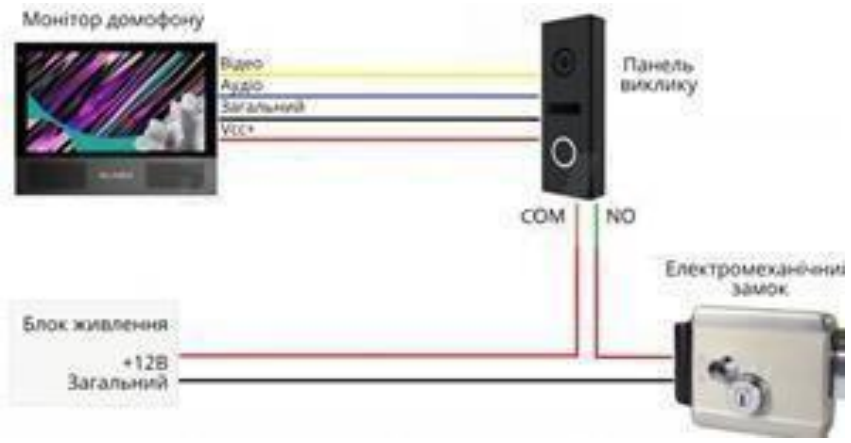

Рисунок 1.4 – Підключення електромеханічного замка до домофона для дистанційного відкривання дверей від блоку живлення

Четвертий варіант – схема 4 відображає сучасний (і найправильніший) варіант підключення відеодомофона та електромеханічного замка (рис. 1.5). Перевагою даної схеми, крім тих, що описані у поясненні до схеми 2, є відсутність необхідності прокладання додаткового кабелю від домофону до панелі виклику – для забезпечення живлення замка.

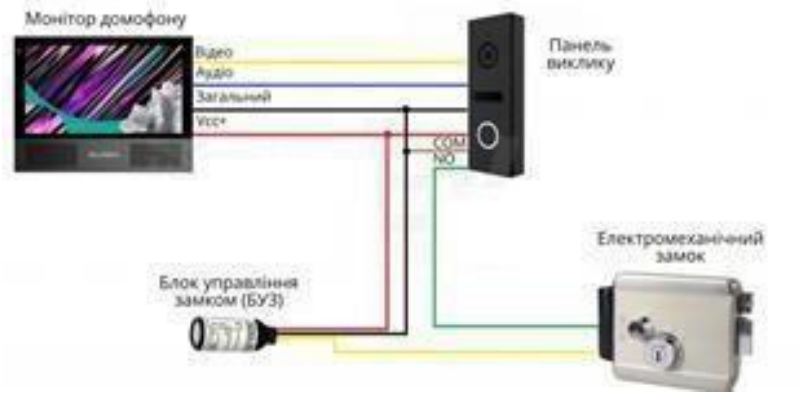

Рисунок 1.5 – Підключення електромеханічного замка до домофона для дистанційного відкриття дверей за допомогою Buz

У сучасних системах контролю доступу електронні замки відіграють ключову роль, пропонуючи широкий спектр рішень для різних потреб. Вибір відповідного типу замка залежить від багатьох факторів, таких як вимоги до безпеки, тип приміщення та особливості використання.

Існує декілька основних видів електронних замків, кожен з яких має свої переваги та сферу застосування.

Тож, проведемо огляд найбільш поширених типів електронних замків, щоб визначитися з їхнім функціоналом та можливостями, а також проаналізувати, які з них найбільше підходять для конкретних умов експлуатації.

Одним із найпоширеніших типів електронних замків є кодові замки (рис. 1.6) [7-9]. Вони працюють на основі введення заздалегідь встановленого коду. Це досить простий у використанні варіант, оскільки користувачеві не потрібно мати при собі фізичний ключ або інший носій для доступу. Здебільшого ці замки знаходять застосування в будівлях, де важлива швидкість і простота доступу, наприклад у багатоквартирних будинках або офісах з великою кількістю користувачів. Однак кодові замки мають і свої недоліки. Наприклад, існує ризик, що зловмисники можуть підібрати код або отримати його іншим способом, тому для забезпечення додаткового захисту важливо регулярно змінювати коди.

Рисунок 1.6 – Кодовий замок

Інший тип електронних замків – це системи, які використовують радіочастотну ідентифікацію (RFID) або магнітні картки (рис. 1.7) [7-9]. У цьому випадку користувач для відкриття замка прикладає картку або брелок

до спеціального зчитувача. Такий підхід є дуже популярним у готелях, офісах та об'єктах з великою кількістю людей. Замки на основі RFID є зручними, адже забезпечують швидкий доступ і можуть бути налаштовані на певний час дії картки, наприклад, для гостьового доступу. Однак ці системи також мають свої недоліки, зокрема ризик втрати або копіювання картки, що може створити загрозу для безпеки об'єкта.

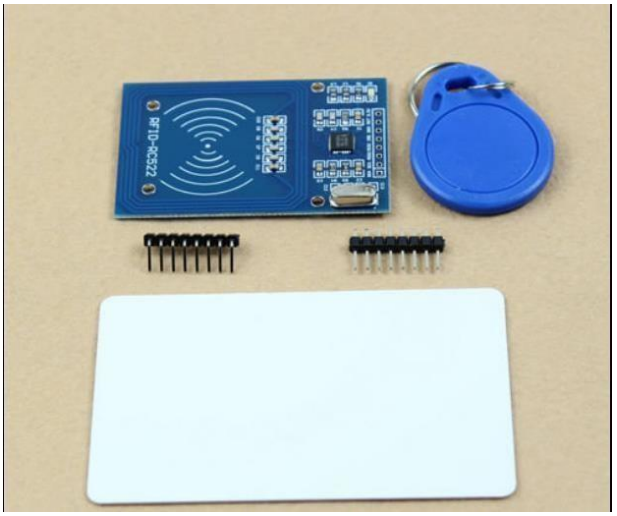

Рисунок 1.7 – RFID замок

Один із найсучасніших і найбільш безпечних варіантів електронних замків – це біометричні системи (рис. 1.8) [7-9]. Біометричні замки працюють на основі розпізнавання унікальних характеристик, таких як відбитки пальців, обличчя або райдужна оболонка ока. Їхня основна перевага – висока безпека, оскільки біометричні дані неможливо втратити чи скопіювати. Часто такі системи поєднуються з іншими методами доступу, такими як паролі або RFID-картки, що підвищує захист. Проте біометричні замки дорожчі за традиційні електронні системи і можуть мати обмеження через помилки розпізнавання, наприклад, через пошкодження шкіри або зміни зовнішнього вигляду.

Рисунок 1.8 – Біометричний замок

Останніми роками значної популярності набувають смарт-замки (рис 1. 9) [7-9], які працюють через мобільні додатки, використовуючи технології Bluetooth або Wi-Fi. Смарт-замки дозволяють користувачам віддалено керувати доступом через смартфон, що зручно для надання доступу іншим особам та моніторингу використання в реальному часі. Вони інтегруються в системи розумного будинку, синхронізуючись з камерами спостереження та системами сигналізації.

Рисунок 1.9 – Wi-fi замок

На додаток до базових типів замків існують комбіновані системи, які поєднують у собі кілька методів автентифікації, таких як введення коду, прикладання картки або використання біометричних даних. Такі рішення дозволяють підвищити безпеку, оскільки користувачам потрібно пройти кілька рівнів захисту для отримання доступу до приміщення. Ці системи найчастіше застосовуються на об'єктах з підвищеними вимогами до безпеки,

таких як банки, урядові установи або великі корпоративні офіси.

Загалом, вибір системи електронного замка залежить від специфіки об'єкта, потреб у безпеці та зручності використання. Кожен тип замка має свої переваги та недоліки, і кінцеве рішення повинно враховувати баланс між вартістю, зручністю та рівнем захисту, необхідним для конкретної ситуації.

1.2 Застосування штучного інтелекту в системах безпеки

Почнемо з огляду методів штучного інтелекту в розпізнаванні користувачів.

Нещодавно інновації в галузі апаратного забезпечення збільшили обчислювальну потужність і створили більше додатків, пов'язаних з штучним інтелектом (ШІ).

Перехід від центральних процесорів до графічних процесорів призвів до підвищення ефективності та розвитку паралельної обробки, а перехід на спеціалізовані ASIC, спеціально розроблені для прискорення методів штучного інтелекту у глибинному навчанні (DL), відчинив двері для рішень локальних та периферійних пристроїв. В результаті багато галузей тепер починають усвідомлювати важливість як апаратного, так і програмного забезпечення при застосуванні ШІ у більш реальних випадках використання.

Від процесорів, графічних процесорів та інтегральна схема для конкретного застосування (ASIC) до модуля обробки даних з технологією глибокого навчання (DLPU) та (система на кристалі) SOC ШІ змінює підхід багатьох виробників пристроїв до дизайну та функціональності майбутніх пристроїв. Незважаючи на те, що ШІ існує вже багато десятиріч, його нещодавні досягнення дозволили технічному співтовариству оптимізувати обчислювальну потужність, необхідну для ШІ та його методів, у тому числі:

– машинне навчання (МН) – підмножина ШІ, яка використовує фундаментальні пізнання та дієві інструменти, алгоритми для вирішення основних проблем шляхом виявлення закономірностей для отримання високонадійних прогнозів, що призводить до прийняття рішень із мінімальним

втручанням людини;

– глибинне навчання (ГН) – підмножина машинного навчання, у якій використовуються алгоритми, засновані на нейронних мережах, що моделюються, натхнені способом навчання людей (і навчені на величезній кількості вхідних даних) для забезпечення більш точних результатів;

– нейронні мережі (NNET) або штучні нейронні мережі (ШНМ) є ядром алгоритмів ГН, структура яких призначена для моделювання роботи людського мозку та його нейронів з метою обробки та розпізнавання взаємозв'язків між даними.

Системи, що базуються на ШІ-технології, враховують найменші аномалії та підозрілу активність. Експерти-люди часто не помічають їх або ж нехтують подібними змінами. Робота ШІ-систем спирається на такі інновації:

– біометрична автентифікація. Застарілі системи безпеки використовували паролі та пін-коди, які легко викрадали шахраї. Системи нового покоління на основі ШІ застосовують персоніфіковані елементи захисту, такі як відбитки пальців, розпізнавання обличчя та голосу, забезпечуючи доступ лише авторизованим користувачам;

– поведінкова біометрія. Штучний інтелект відкриває нові можливості для систем безпеки та шахраїв. Системи на основі ШІ потребують даних поведінкової біометрії – індивідуальної «цифрової поведінки» користувачів, як-от манера набору тексту чи гортання сторінок. ШІ аналізує ці патерни для захисту облікових записів;

– транзакційна поведінка. Класичні системи безпеки використовують запрограмовані правила для виявлення аномальних транзакцій, але часто викликають хибні спрацьовування. ШІ-механізми на основі машинного навчання автономно збирають поведінкові патерни користувача, знижуючи кількість помилок і незручностей;

– обробка природної мови. Інтеграція чат-ботів і віртуальних помічників спрощує грошові перекази через розмовний інтерфейс. Алгоритми обробки природної мови допомагають виявляти примус і шахрайство,

підвищуючи безпеку платежів і покращуючи взаємодію з користувачем.

Далірозглянемо ключові етапи ШІ-систем для виявленняшахрайства. рис. 1.10 [10, 11].

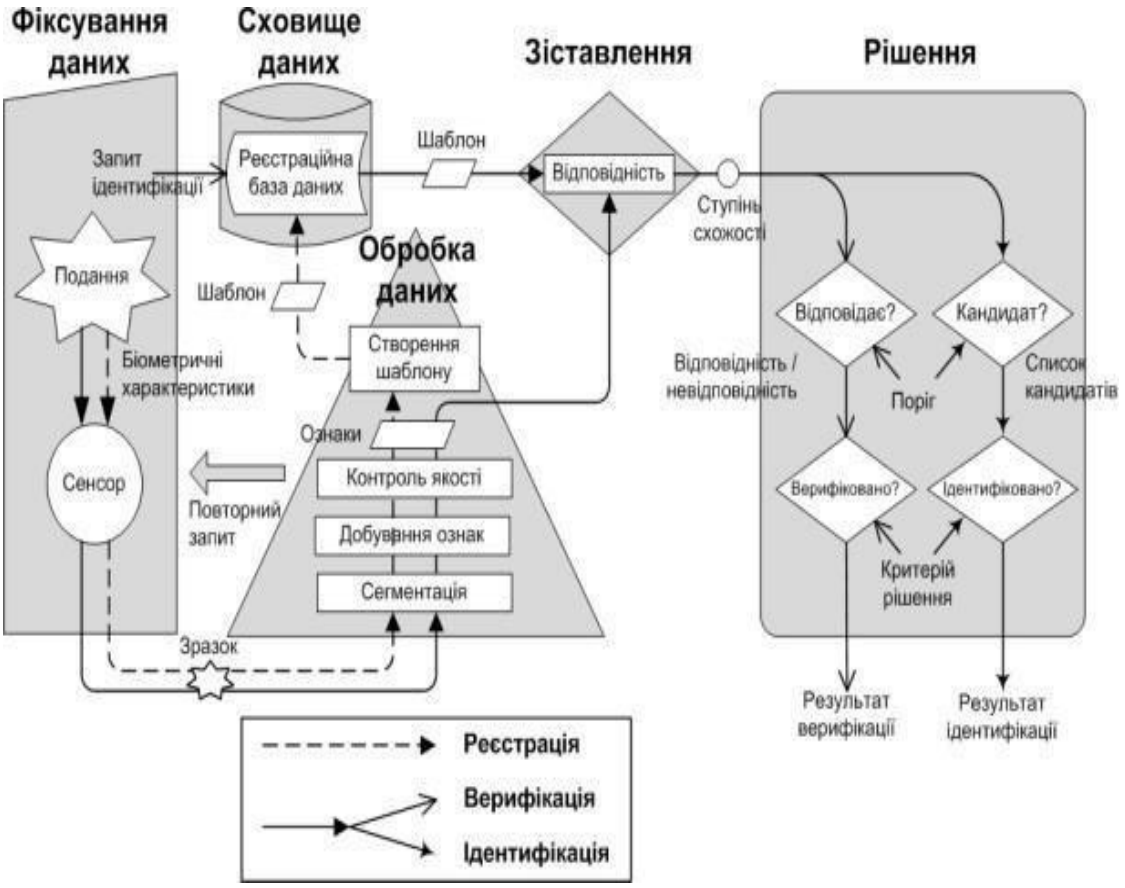

Рисунок 1.10 – Схематичне зображення механізму попередження шахрайства

Механізми попередження шахрайства, що побудовані на основі ШІ-технологій, складаються з наступних етапів:

– фіксування даних. Точні та якісні дані слугують ядром ШІ-систем, покликаних запобігати випадкам шахрайства. Потрібно забезпечити доступ до транзакційних та поведінкових даних, отриманих з різних джерел;

– розуміння шахрайської поведінки. Наступний етап полягає в ідентифікації певних рис та патернів, які маркують поведінку шахраїв. Система на базі штучного інтелекту вирізняє поведінкові моделі авторизованого користувача та шахрая;

– тренування моделі. Коли система отримує достатньо даних і запам’ятовує поведінкові патерни авторизованих користувачів та зловмисників, алгоритми починають застосовувати в реальних умовах. Використовуються історичні дані, в яких треновані моделі виявляють випадки шахрайства;

– виявлення аномалій. Система спирається на запрограмовані алгоритми та інформує про виявлення аномальної поведінки;

– постійне оновлення. Моделі на основі машинного навчання потребують безперервного завантаження нових даних та патернів задля можливості протистояти видозміненим і оновленим шахрайським механізмам;

– сповіщення та звіти. Як тільки система виявляє поведінку, що виходить за межі шаблонної поведінки авторизованого користувача, вона повідомляє про підозрілу активність і надсилає деталізовані звіти для більш глибокого розслідування ситуації.

Таким чином ШІ-моделі, розроблені для попередження шахрайства, потребують великих обсягів даних, тренування та безперервного навчання для забезпечення потреб систем безпеки платежів.

Наступним пунктом розглянем використання нейронних мереж для контролю доступу.

У світі нейронних мереж для аналізу зображень, несумнівно, відбувається бурхливий розвиток. Однак, щоб максимізувати їхній потенціал і вдосконалити результати аналізу зображень, важливо вдосконалювати та оптимізувати процеси. Розглянемо деякі з можливостей оптимізації та покращення результатів з використанням нейронних мереж:

– попередня обробка зображень є важливим кроком перед їхнім введенням у нейронну мережу, тому застосування фільтрів, нормалізація, аугментація та інші техніки можуть покращити якість та інформаційність зображень, зменшити шум та підготувати дані для навчання та тестування;

– вибір правильної архітектури нейронної мережі та гіперпараметрів є вирішальним завданням тож деякі завдання можуть вимагати глибоких ме-

реж, тоді як інші – менше кількості параметрів для досягнення найкращих результатів;

– використання заздалегідь навчених моделей та їх докладання для вирішення конкретних завдань може значно зекономити час і ресурси. Fine-tuning дозволяє адаптувати модель до нових завдань, використовуючи знання, набуті на попередніх наборах даних;

– комбінування декількох моделей, таких як декілька CNN, може покращити результати аналізу зображень, ансамблі також можуть підвищити точність та зменшити ризик перенавчання;

– нові інновації в архітектурах, такі як архітектура Transformer для обробки послідовностей, можуть бути адаптовані для аналізу зображень і приз- вести до покращення результатів;

– використання апаратного прискорення, такого як графічні процесори (GPU) та тензорні процесори (TPU), допомагає покращити продуктивність нейронних мереж та дозволяє обробляти великі обсяги даних швидше.

Оптимізація та покращення результатів аналізу зображень з використанням нейронних мереж є безперервним процесом, і вона відіграє важливу роль у покращенні продуктивності та точності цих систем. Наявність нових технологій та підходів в цій галузі надає великі можливості для подальших досліджень та розвитку. Розглянемо більш детальний приклад оптимізації процесу виявлення об’єктів на зображенні, побудований на основі вище згаданих можливостей оптимізації та покращення результатів з використанням нейронних мереж. В цьому підході було використано існуючу модель YOLOv5 та введено певні модифікації в методи цієї моделі. Схема роботи такої системи наведена на рис. 1.11 [10,11].

Традиційні методи верифікації особи, що базуються на паролях і ключових даних, часто є ненадійними і незручними через можливість їх втрати чи забування.

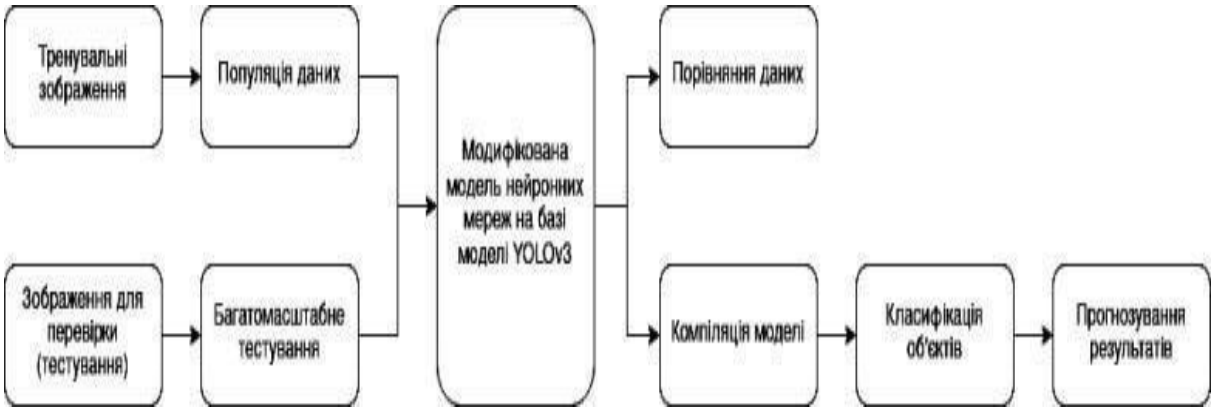

Рисунок 1.11 – Модель на базі YOLOv5

Для підвищення надійності автентифікації стало популярним використання біометричних технологій. Наразі біометричні системи застосовуються для контролю фізичного доступу та доступу до інформації на різних рівнях: приватному, корпоративному, державному та міждержавному.

Однак існує суттєва різниця між ефективністю біометричних методів у лабораторних умовах, заявленою розробниками, і результатами незалежного тестування.

Розглянемо стандарти, що визначають цю ієрархію, та організації, які займаються їх створенням.

Ієрархію стандартів з біометрії наведено на рис. 1.12 [10,12].

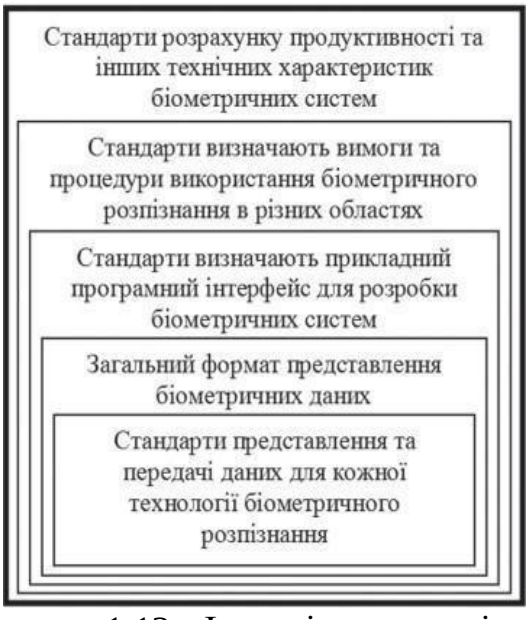

Рисунок 1.12 – Ієрархія стандартів з біометрії

Використання відбитків пальців для ідентифікації спирається на контрольні точки, розташовані в місцях закінчення або біфуркації гребенів. Опис їх розташування й орієнтації дозволяє визначити, чи є два відбитки від одного пальця. Існує два основних типи контрольних точок: точка закінчення та точка біфуркації гребеня. Іноді зустрічаються складніші точки, що є комбінацією основних типів. Додаткові точки, які не є закінченням або біфуркацією, класифікуються як "інші контрольні точки". Таким чином, цей стандарт встановлює наступні типи контрольних точок:

– закінчення гребеня (точка біфуркації основи западин);
– біфуркація гребеня;
– інша контрольна крапка.

У залежності від методу визначення положення точки допускається визначати контрольну точку закінчення гребеня як точку біфуркації западини. Основу западини обчислюють поетапним зменшенням площі западини до лінії шириною в один елемент зображення. У системі координат зображення пальця вісь X повинна бути направлена справа наліво відповідно до рис. 1.13 [6]. Всі значення координат X і Y повинні бути невід’ємними.

Рисунок 1.13 – Система координат

У ході проведеного огляду, можна визначити переваги та недоліки ШІ у порівнянні з традиційними методами.

Сфери застосування штучного інтелекту безмежні і охоплюють різні галузі. У охороні здоров'я ШІ використовується для дозування ліків, вибору методів лікування та підтримки хірургічних процедур. Інші приклади включають комп’ютери, що грають у шахи, та безпілотні автомобілі, які повинні враховувати наслідки своїх дій. У шахах це перемога в партії, а в безпілотних автомобілях – уникнення зіткнень, враховуючи всі зовнішні дані.

Переваги штучного інтелекту:

– підвищення ефективності та автоматизації. ШІ має вирішальне значення для підвищення операційної ефективності за рахунок автоматизації. Це прискорює процеси та мінімізує помилки, що призводить до значного підвищення загальної продуктивності, оптимізації робочих процесів і поліпшенню розподілу ресурсів в організаціях;

– аналіз даних та інсайти. Сучасний бізнес працює в умовах змінної інформації. Штучний інтелект аналізує великі масиви даних, виявляє закономірності та надає цінну інформацію для стратегічного планування і покращення бізнес-аналітики;

– персоналізація та клієнтський досвід. ШІ змінив взаємодію компаній з клієнтами, забезпечивши персоналізований досвід. Аналізуючи поведінку користувачів, системи адаптують рекомендації та послуги, підвищуючи задоволеність і лояльність, що є важливим у конкурентному середовищі;

– інновації та творчість. Штучний інтелект стимулює інновації, автоматизуючи рутинні завдання та вивільняючи людський потенціал для творчості. Взаємодія ШІ з людською креативністю розширює можливості у сфері дизайну, вирішення проблем та генерування ідей;

– скорочення витрат і оптимізація ресурсів. Автоматизація процесів за допомогою ШІ дозволяє бізнесу знизити витрати на робочу силу, підвищити операційну ефективність і оптимізувати ресурси. Це робить ШІ важливим інструментом для максимізації ефективності та збереження фінансової стійкості;

– посилення безпеки та виявлення шахрайства. Штучний інтелект

зміцнює кібербезпеку, аналізуючи транзакції та виявляючи загрози в реальному часі. Проактивний підхід підвищує стійкість бізнесу до кіберзагроз і захищає від фінансових ризиків;

– автономні системи. Розробка автономних систем на базі штучного інтелекту змінює парадигму в різних галузях, таких як транспорт, логістика та виробництво. Вони підвищують безпеку, зменшуючи людські помилки, покращують операційні можливості та відкривають нові горизонти в сферах, де важливі точність, ефективність і надійність;

– мовний переклад і комунікація. Інструменти перекладу на базі штучного інтелекту подолали мовні бар'єри, забезпечуючи спілкування в реальному часі. Це дозволяє компаніям ефективніше взаємодіяти з міжнародною аудиторією, сприяючи співпраці та розширенню ринків. ШІ покращує комунікацію та відкриває нові можливості у глобальній бізнес-взаємодії.

Основні недоліки використання штучного інтелекту:

– високі початкові витрати. Інтеграція штучного інтелекту в бізнес вимагає значних початкових інвестицій у технології, інфраструктуру та кваліфікованих фахівців. Малі та середні підприємства можуть вважати ці витрати непомірно високими, що стає перешкодою для впровадження; заохочення людських лінощів. ШІ робить людей лінивими, автоматизуючи рутинні завдання. Це може викликати самозаспокоєння, знижуючи схильність до активної участі у вирішенні проблем, критичного мислення та прагнення до вдосконалення;

– втрата робочих місць і проблеми з працевлаштуванням. Можливості ШІ в автоматизації підвищують ефективність, але викликають занепокоєння щодо втрати робочих місць. Зменшення втручання людини може погіршити стандарти зайнятості, оскільки рутинні завдання легко автоматизуються, що знижує шанси на працевлаштування. Організації прагнуть замінити малокваліфікованих працівників ШІ, який виконує роботу ефективніше;

– відсутність емоцій. Хоча машини ефективні у виконанні завдань, во-

ни не можуть замінити людський зв'язок у команді. Обмеження ШІ в розумінні складного людського контексту, емоцій, культурних нюансів і соціально-етичних дилем створює проблеми в ситуаціях, де глибоке розуміння є важливим для прийняття рішень;

– відсутність нестандартного мислення. Незважаючи на майстерність в обробці даних, ШІ позбавлений творчих здібностей і інтуїції людини в прийнятті рішень. Машини виконують лише завдання, на які вони спроектовані, і все, що виходить за межі цього, може призвести до збоїв або нерелевантних результатів;

– проблеми залежності та надійності. Надмірна довіра до систем штучного інтелекту може призвести до залежності та ризиків. Помилки в ШІ можуть викликати операційні збої, ставлячи під сумнів надійність процесів. Важливо досягти балансу, щоб ШІ доповнював людські здібності, не загрожуючи стійкості системи.

Отже, розглянувши методи штучного інтелекту у розпізнаванні користувачів я визначив що ШІ значно підвищує ефективність та безпеку систем автентифікації. ШІ відкриває нові горизонти у розпізнаванні за допомогою біометрії, поведінкових ознак та аналізу транзакційної активності, що робить його незамінним інструментом у сучасних технологіях захисту даних.

Проєкт дозволить дослідити сучасні методи машинного навчання, нейронних мереж та обробки зображень, а також їх інтеграцію з мікроконтролерами. Використання таких технологій робить тему актуальною та перспективною, оскільки електронні замки з ШІ вже набирають популярності на ринку. Це відкриває можливості для подальшого розвитку системи, наприклад, для інтеграції з іншими елементами розумного дому або розробки комерційного продукту.

1.3 Огляд цифрових замків з штучним інтелектом

У ході роботи розглянуто основні характеристики кодового дверного замку Philips Easy Key Alpha (рис. 1.14): цифрова клавіатура із сенсорним керуванням; автоматична система блокування; чорний корпус сучасного дизайну; можливість відкриття за допомогою коду; вбудована система безпеки [7].

Також наведено переваги: зручність використання – не потрібні фізичні ключі; автоматичне закривання дверей; сучасний дизайн; надійна система безпеки; простота встановлення та використання; сенсорне управління.

Також визначено основні недоліки: залежність від елементів живлення; вища вартість у порівнянні з механічними замками; необхідність періодичної заміни батарей; можливі складності при екстремально низьких температурах; ризик забування коду доступу.

Рисунок 1.14 – Кодовий дверний замок Philips Easy Key Alpha [7]

У ході роботи розглянуто основні характеристики Philips Easykey DDL702E (рис. 1.15): розумний замок; Wi-Fi; функції доступу (створення та керування кодами доступу віддалено); підтримка різних способів відкриття (наприклад, смартфон, код, ключ); отримання повідомлень про доступ та зміну статусу замку; підтримка роботи з програмами для мобільних

пристроїв; інтуїтивно зрозумілий інтерфейс для керування замком; високий рівень шифрування та захист доступу [7].

Рисунок 1.15 – Smart lock замок Philips Easykey DDL702E [7]

З огляду на замок визначено наступні переваги: можливість керувати замком з будь-якої точки світу робить його зручним для власників, які часто знаходяться далеко від дому; підтримка різних методів доступу дозволяє вибрати найзручніший варіант для користувача; повідомлення в реальному часі; широка підтримка мобільних додатків полегшує використання замку та керування ним; удосконалені системи шифрування забезпечують захист від несанкціонованого доступу.

Також основними недоліками замку є: залежність від Wi-Fi (якщо Wi-Fi сигнал нестабільний або відсутній, керування замком може стати скрутним) енергоспоживання (розумні замки можуть вимагати регулярної заміни батарей або заряджання, що може бути незручно); вартість(розумні замки часто коштують дорожче за традиційні замки, що може бути перешкодою для деяких покупців); уразливість(як і будь-який IoT-пристрій, розумний замок може бути схильний до хакерських атак, якщо не дотримуються заходів безпеки); системні збої (можливі проблеми з програмним забезпеченням можуть призвести до неправильної роботи пристрою).

У ході роботи розглянуто основні характеристики Philips Easykey 7300 (рис. 1.16): тип замку (цифровий замок); дизайн (елегантний та простий, компактний та тонкий); підтримка різних методів (код, ключ, мобільний додаток); управління (інтуїтивно зрозумілий інтерфейс); безпека (високий рівень захисту та шифрування); установка (легка установка, підходить для більшості дверей) [7].

Рисунок 1.16 – Цифровий замок Philips Easykey 7300 [7]

З огляду на замок визначено наступні переваги: компактність (тонкий та елегантний дизайн дозволяє економити місце та гармонійно вписується в інтер'єр); зручність у використанні (різноманітність способів доступу робить замок зручним для різних користувачів); простота установки (легке встановлення дозволяє швидко замінити старий замок без необхідності виклику фахівця); безпека (високий рівень захисту забезпечує надійність та захист від несанкціонованого доступу); сучасний дизайн (естетично привабливий вигляд замку може покращити зовнішній вигляд дверей).

Також основними недоліками замку є: залежність від джерела живлення (цифрові замки можуть вимагати заміни батарей, що може бути незручно); вартість (цифрові замки можуть бути дорожчими за традиційні, що може обмежити вибір для деяких користувачів); уразливість до хакерських атак (як і інші розумні пристрої, замок може бути схильний до кіберзагроз, якщо не дотримуються заходів безпеки); складнощі програмного забезпечення

(можливі збої в роботі програмного забезпечення можуть призвести до проблем з доступом); необхідність навчання (користувачам може знадобитися час для звикання до нового пристрою та його функцій).

У ході роботи розглянуто основні характеристики Kaadas K9 Black (рис. 1.17): тип замку (електрозамок із функцією відбитка пальця); метод доступу (відбиток пальця, ключ, мобільний додаток); дизайн (сучасний та стильний, з ручкою Push-Pull); встановлення (підходить для більшості дверей, легке встановлення); безпека (високий рівень захисту, шифрування даних); додаткові функції (можливість керування через мобільний додаток) [7].

Рисунок 1.17 – Електрозамок Kaadas K9 Black з відбитком пальцю [7]

З огляду на замок визначено наступні переваги: зручність використання (швидкий доступ за допомогою відбитка пальця, що унеможливлює ключі); сучасний дизайн (естетично привабливий вигляд, що підходить до будь-якого інтер'єру); технологія Push-Pull (зручна ручка, що дозволяє легко відчиняти двері) багатофункціональність (підтримка кількох методів доступу для зручності користувачів); безпека (високий рівень захисту від несанкціонованого доступу).

Також основними недоліками замку є: залежність від джерела живлення (необхідність батарей, які можуть вимагати заміни); вартість (електрозамки можуть бути дорожчими за традиційні замки); вразливість до збоїв (можливі проблеми з програмним забезпеченням можуть призвести до збоїв у роботі); необхідність навчання (користувачам може знадобитися час для звикання до нових функцій); обмежена робота в умовах низьких температур (деякі моделі можуть не працювати належним чином під час сильного морозу).

1.4 Висновки до розділу 1

В даному аналізі розглянуто принципи роботи та особливості встановлення електричних замків, а також здійснено огляд різних типів електронних замків. Це дослідження допомагає зрозуміти основні механізми та переваги електричних замків у системах контролю доступу, а також підкреслює важливість правильного монтажу для забезпечення їх безпеки та надійності. Вивчення різних типів замків, таких як кодові, RFID, біометричні та смарт-замки, дозволяє створити основу для вибору найбільш підходящого рішення залежно від конкретних вимог до безпеки, зручності використання та технологічних вподобань. Це дослідження є важливим для прийняття обґрунтованих рішень при впровадженні ефективних та надійних систем контролю доступу в різних сферах, від житлових до комерційних і високозахищених об'єктів. Аналіз типів замків також показує, що важливим є баланс між безпекою, зручністю і витратами при впровадженні електронних замкових систем.

2 РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЕЛЕКТРОННИМ ЗАМКОМ

2.1 Аналіз вимог до систем електронних замків з використанням штучного інтелекту

Вимоги до системи захисту інформації.

Закордонний і вітчизняний досвід показує, що для забезпечення виконання багатогранних вимог безпеки система захисту інформації повинна задовольняти такі умови:

– охоплювати весь технологічний комплекс інформаційної діяльності;

– бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу;

– бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;

– бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;

– бути простою для технічного обслуговування і зручною для експлуатації користувачами;

– бути надійною, тобто, будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації;

– бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієїсистеми.

До системи безпеки інформації висуваються також певні вимоги:

– чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;

– надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;

– зведення до мінімуму кількості спільних для декількох користувачів

засобів захисту;

– облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;

– забезпечення оцінювання ступеня конфіденційної інформації;

– забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

Розглянемо основні види забезпечення системи захисту інформації. Функціональні вимоги, які мають виконувати електронні замки:

– основна функція електронних замків – забезпечити обмежений доступ до приміщень, дозволяючи його лише авторизованим особам;

– після закриття дверей замок може автоматично заблокуватися, що забезпечує додатковий рівень безпеки, навіть якщо користувач забуде про це;

– замки можуть бути налаштовані для роботи в різних режимах, включаючи тимчасовий доступ для певних користувачів, індивідуальні розклади доступу (наприклад, для працівників), або ж інтеграцію з системами «розумного дому»;

– багато електронних замків фіксують усі спроби доступу, дозволяючи адміністратору відстежувати, хто і коли входив або намагався увійти в приміщення;

– електронні замки можуть бути частиною більш складних систем безпеки, включаючи відеоспостереження, сигналізації або автоматизовані системи управління будівлею;

– більшість замків мають можливість аварійного відкриття у разі технічних проблем, як-от збій живлення або пошкодження;

– деякі електронні замки дозволяють власнику контролювати доступ дистанційно за допомогою мобільних додатків або інших інтернет-засобів, відкривати двері або перевіряти статус замка.

Нефункціональні вимоги для електронних замків визначають їх якісні характеристики, такі як надійність, безпека, продуктивність та зручність використання. Замок повинен стабільно працювати без збоїв та мати резервне

живлення при відключенні електроенергії. Важливо забезпечити високий рівень безпеки, захищаючи від злому, хакерських атак та перехоплення сигналів через шифрування даних і багатофакторну аутентифікацію.

Продуктивність замка має забезпечувати швидку реакцію на запити доступу та миттєве блокування чи розблокування. Також важливою є масштабованість для додавання нових користувачів без втрати ефективності, особливо в великих будівлях.

Зручність використання включає простоту встановлення та експлуатації, швидкий і інтуїтивно зрозумілий процес додавання або видалення користувачів. Замок повинен бути сумісний з системами управління доступом, такими як «розумний дім», і підтримувати різні типи пристроїв доступу.

Електронний замок має бути стійким до зовнішніх факторів, енергоефективним з мінімальним споживанням енергії, і сповіщати про низький рівень заряду батареї. Важливою характеристикою є простота обслуговування та ремонту, а також можливість швидкого оновлення програмного забезпечення, забезпечуючи високий рівень доступності з мінімальним часом простою.

Загальною метою GDPR є забезпечення високого рівня захисту особистих даних клієнтів, а саме запобігання витоку даних. Виконання цих стандартів сприяє покращенню довіри клієнтів та зменшенню ризику порушень конфіденційності персональної інформації клієнтів. Нижче буде перераховано ключові аспекти безпеки, які мають враховуватися організаціями для досягнення відповідності GDPR.

Укладання угод з обробниками даних. GDPR вимагає укладати відповідні угоди, в яких встановлюються вимоги щодо безпеки і захисту особистої інформації, якщо ви передаєте особисті дані обробникам:

– забезпечення найновішого захисту. Організації повинні мати обізнаність та регулярно оновлювати та захищати свої інформаційні системи та програмне забезпечення від всіляких загроз;

– шифрування даних. Важливим засобом захисту є шифрування, яке

повинно здійснюватися при передачі чи в процесі зберігання особистих даних. Це допомагає захистити дані від несанкціонованого доступу та витоку інформації;

– захист від порушень. GDPR вимагає від організацій приділяти особисту увагу захисту персональної інформації від порушень. Організації повинні впроваджувати політику виявлення і реагування за порушення безпеки даних;

– передача особистих даних. При передачі особистих даних клієнтів, особливо за межами Європейського союзу, обов'язково слід використовувати захист та шифрування відповідно до умов регламенту;

– тренінг та усвідомлення персоналу. Забезпечення того, що персонал розуміє важливість безпеки даних та вимог GDPR, є критично важливим.

Загалом, дотримання регламенту вкрай важливе для збереження довіри клієнтів та бізнесу. Дотримання конфіденційності зменшує ризики порушення безпеки даних, таких як витік інформації, крадіжка, несанкціонований доступ або передача особистих даних третім особам.

У даному розділі проведено детальний аналіз існуючих систем електронних замків та особливостей їх встановлення. Розглянуто принципи роботи електрозамків, які за своєю суттю є виконавчими елементами системи контролю та управління доступом (СКУД). Досліджено різні типи електрозамків: нормально замкнені, нормально відімкнені та універсальні, кожен з яких має свої особливості функціонування залежно від подачі електричного сигналу.

Особлива увага приділена схемам підключення електромеханічних замків. Детально розглянуто чотири варіанти монтажу: від найпростішої схеми з блоком живлення до сучасних рішень з використанням блоків управління замком (БУЗ). Проаналізовано переваги та недоліки кожної схеми підключення, що допомагає обрати оптимальний варіант для конкретних умов застосування.

У документі також представлено огляд основних типів електронних замків, включаючи кодові замки, системи з RFID-технологією, біометричні системи та смарт-замки з Wi-Fi підключенням. Для кожного типу замків описано принципи роботи, сфери застосування, переваги та потенційні недоліки.

Мета цього аналізу полягає в тому, щоб надати повне розуміння сучасних систем електронних замків, допомогти у виборі оптимального рішення для конкретних потреб, враховуючи такі фактори як безпека, зручність використання, надійність та вартість. Такий комплексний огляд особливо важливий для спеціалістів, що займаються проектуванням та встановленням систем контролю доступу, а також для користувачів, які прагнуть зробити обґрунтований вибір системи безпеки для свого об'єкта.

2.2 Розроблення структурної схеми системи управління складним електронним замком

У ході роботи було запропоновано узагальнену структурну схему системи. Пристрій введення (клавіатура) – це інтерфейс, через який користувач вводить код доступу, щоб розблокувати електромеханічний замок. Клавіатура може бути як механічною, так і сенсорною.

Датчик відкриття дверей – цей датчик визначає, чи двері відкриті або закриті. Він може бути магнітним або механічним і відправляє сигнал мікроконтролеру про стан дверей.

Виконавчий елемент електромеханічного замка – це пристрій, який фізично замикатиме та розмикатиме замок на дверях. Він активується мікроконтролером на основі введеного коду.

Мікроконтролер – центральний елемент системи, який обробляє дані з клавіатури, аналізує введений код, керує виконавчими елементами та обробляє сигнали від датчиків.

Пристрій сигналізації про відкриття дверей – це система, яка сповіщає

про те, що двері були відкриті. Вона може використовувати звукові сигнали, світлові індикатори або посилати повідомлення на телефон.

Пристрій сигналізації про спробу підбору коду – цей блок виявляє несанкціоновані спроби вводу коду (наприклад, кілька невдалих спроб) і активує сигналізацію, щоб попередити про можливе злоумисне втручання.

Ця схема працює в комплексі, забезпечуючи безпеку та контроль доступу до приміщення, зображена на рис. 2.1.

Рисунок 2.1 – Узагальнена структурна схема системи

Додатково, система може бути інтегрована з мобільними додатками для віддаленого контролю, що дозволяє користувачам моніторити стан дверей та отримувати сповіщення про події в реальному часі. Можливість налаштування інтерфейсу та звукових сигналів забезпечує адаптацію системи під потреби користувачів. Всі ці елементи функціонують у комплексі, забезпечуючи ефективну безпеку та контроль доступу до приміщення.

2.3 Вибір компонентів апаратної частини

Для реалізації проекту обрано мікроконтролер ATmega328P-PU, який використовується в платі Arduino Uno R3. Ця плата ідеально підходить для нашого проекту завдяки вбудованому програматору, підтримці шини I2C та компактному форм-фактору, що спрощує складання та налаштування пристрою.

Розглянемо основні компоненти.

Основна плата Arduino Uno. Arduino Uno служитиме основним контролером системи, забезпечуючи обробку даних та управління всіма компонентами.

Модулі безпеки. Для забезпечення безпеки системи можна використовувати модулі, які виконують додаткові функції, такі як датчики руху, мікрофони для виявлення звуків та камери для відеоспостереження.

Магнітні датчики. Вони складаються з двох частин – магніту та датчика, що дозволяє виявляти, коли двері відчинені або закриті.

Механічні датчики. Використовують фізичний контакт для визначення стану дверей.

Блок живлення. Для живлення системи можна використовувати: Адаптер живлення він забезпечує постійне живлення від електромережі.

Акумулятор потрібен для автономної роботи системи, що дозволяє використовувати її в умовах відсутності електрики. У рамках роботи було обрано блок живлення.

Зарядний модуль. Якщо в системі використовуються акумулятори, важливо інтегрувати модулі для заряджання. Це дозволить зручно підзаряджати акумулятори без демонтажу.

LCD дисплей буде використовуватися для відображення статусу замка, введення пароля або ідентифікаційного коду. Це дозволить користувачеві бачити інформацію про стан системи та здійснювати взаємодію з нею.

Клавіатура потрібна для введення пароля система потребує клавіатури.

Це може бути матрична клавіатура, що дозволяє вводити коди доступу для відкриття замка.

Світлодіоди будуть використовуватися для візуальної індикації статусу замка (відчинено/закрито, активний/неактивний). Це дозволить швидко визначити стан системи. На рисунку 2.2 представлена узагальнена електрона схема з підключенням компонентів.

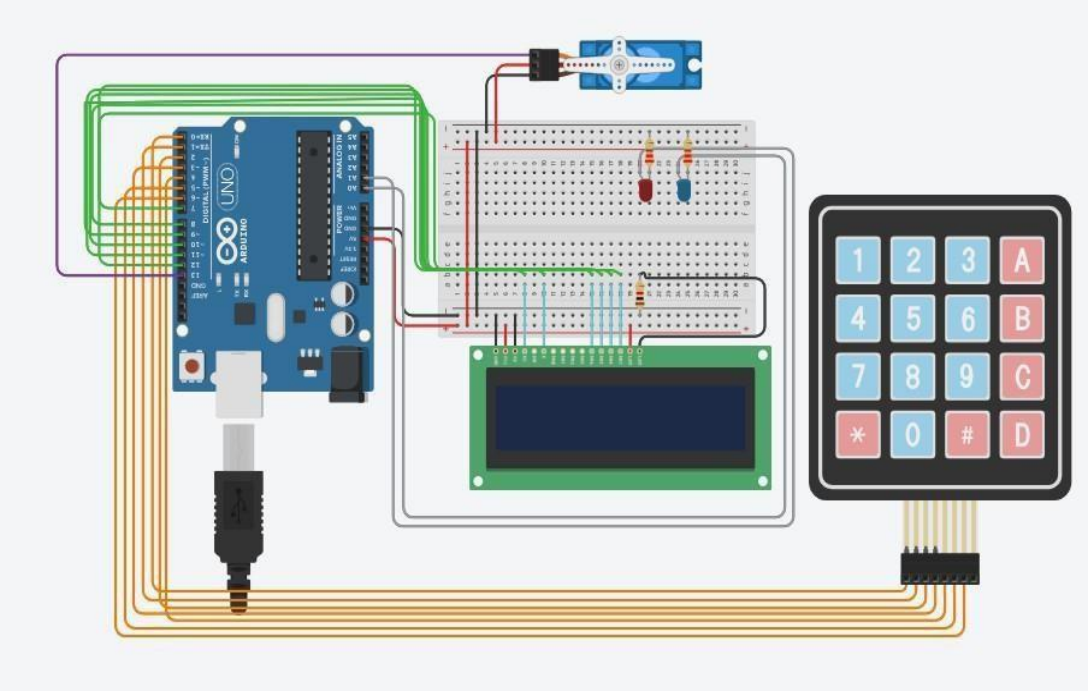

Рисунок 2.2 – Узагальнена електрона схема

Проект починається з підключення клавіатури до Arduino. Перед тим, як перейти до деталей, ретельно планується, як найкраще організувати всі з’єднання, щоб уникнути помилок у подальшій роботі. Ряд 1 (R1) підключається до порту D2, що забезпечує швидкий доступ до першого ряду кнопок. Ряд 2 (R2) підключається до порту D3, ряд 3 (R3) – до порту D4, а ряд 4 (R4) – до порту D5. Стовпці клавіатури підключаються наступним чином: стовпець 1 (C1) з’єднується з D6, стовпець 2 (C2) – з D7, стовпець 3 (C3) – з D8, а стовпець 4 (C4) – з D9. Цей етап важливий, адже клавіатура слугує основним інтерфейсом для взаємодії з користувачем.

Далі переходимо до підключення LCD дисплея, який дозволяє

відображати інформацію та статуси. SDA підключається до порту A4 на Arduino, а SCL – до порту A5. Це значно спрощує підключення, адже не потрібно вести багато дротів до дисплея.

Наступним кроком є підключення реле, яке дозволяє контролювати електронний замок. Сигнальний пін реле (IN) підключається до порту D10 на Arduino, що забезпечує управління його станом. Один контакт реле з'єднується з живленням електронного замка, а інший – з землею. Це важливо для коректної роботи реле, адже воно виконуватиме команду замикання або розмикання електричного кола.

На з'єднанні живлення для всіх компонентів. GND (землю) від усіх компонентів підключають до GND на Arduino, що є критично важливим для стабільної роботи всієї системи. VCC (живлення) всіх компонентів також підключається до +5V на Arduino.

Після того, як всі компоненти підключені, перевіряємо кожне з'єднання, щоб переконатися, що все виконано правильно. Це важливий момент, адже належне підключення – запорука успішної роботи проекту. Тепер переходимо до наступного етапу: програмування Arduino для взаємодії з клавіатурою, дисплеєм і реле. Для того щоб, можна було реалізувати різноманітні функції, такі як введення коду, відображення інформації на дисплеї та контроль електронного замка в залежності від введених даних.

2.4 Розроблення алгоритму роботи системи управління складним електронним замком

Електронний замок працює за основним алгоритмом, який розпочинається з ініціалізації системи. На цьому етапі відбувається налаштування RFID зчитувача, що передбачає встановлення швидкості передачі даних та підключення до мікроконтролера. Паралельно налаштовується сервопривід, що включає тестування його працездатності і налаштування позицій для відкриття та закриття замка. Також ініціалізуються

LED індикатори: зелений та червоний, а зумер настроюється для подачі звукових сигналів.

Після завершення ініціалізації система переходить до основного циклу роботи. У цьому циклі електронний замок постійно чекає на піднесення картки до RFID зчитувача. Коли картка піднесена, система перевіряє її валідність, порівнюючи з базою даних дозволених карток. На основі результату перевірки з'являються два можливі сценарії: успішна або неуспішна авторизація. Якщо картка виявилася валідною, то система активує сервопривід для відкриття замка і увімкне зелений LED індикатор. Одночасно запускається таймер на 5 секунд, по закінченні якого замок автоматично закривається. У разі неуспішної авторизації включається червоний LED індикатор та активується звуковий сигнал зумера, який триватиме 2 секунди.

Система також має можливість виходу з приміщення за допомогою кнопки, що знаходиться всередині. У разі натискання на цю кнопку замок відкривається, і активується зелений LED індикатор.

До основного функціоналу можуть бути додані кілька корисних функцій. Наприклад, ведення журналу доступу, який реєструє всі спроби входу (як успішні, так і неуспішні) з зазначенням часу та детальної інформації про спроби. Також можна впровадити часові обмеження для дозволу або заборони доступу в певні періоди, наприклад, тільки в робочі години. Крім того, система може включати механізм аварійного відкриття замка, що дозволяє фізично відкрити замок у випадку електронних збоїв або відсутності живлення. Нарешті, можливе підключення до Wi-Fi для віддаленого керування замком, завдяки чому користувач зможе моніторити стан замка та відкривати його через мобільний додаток з певними правами доступу [10].

На рис. 2.3 зображено узагальнену блок схему алгоритму роботи електронного замка.

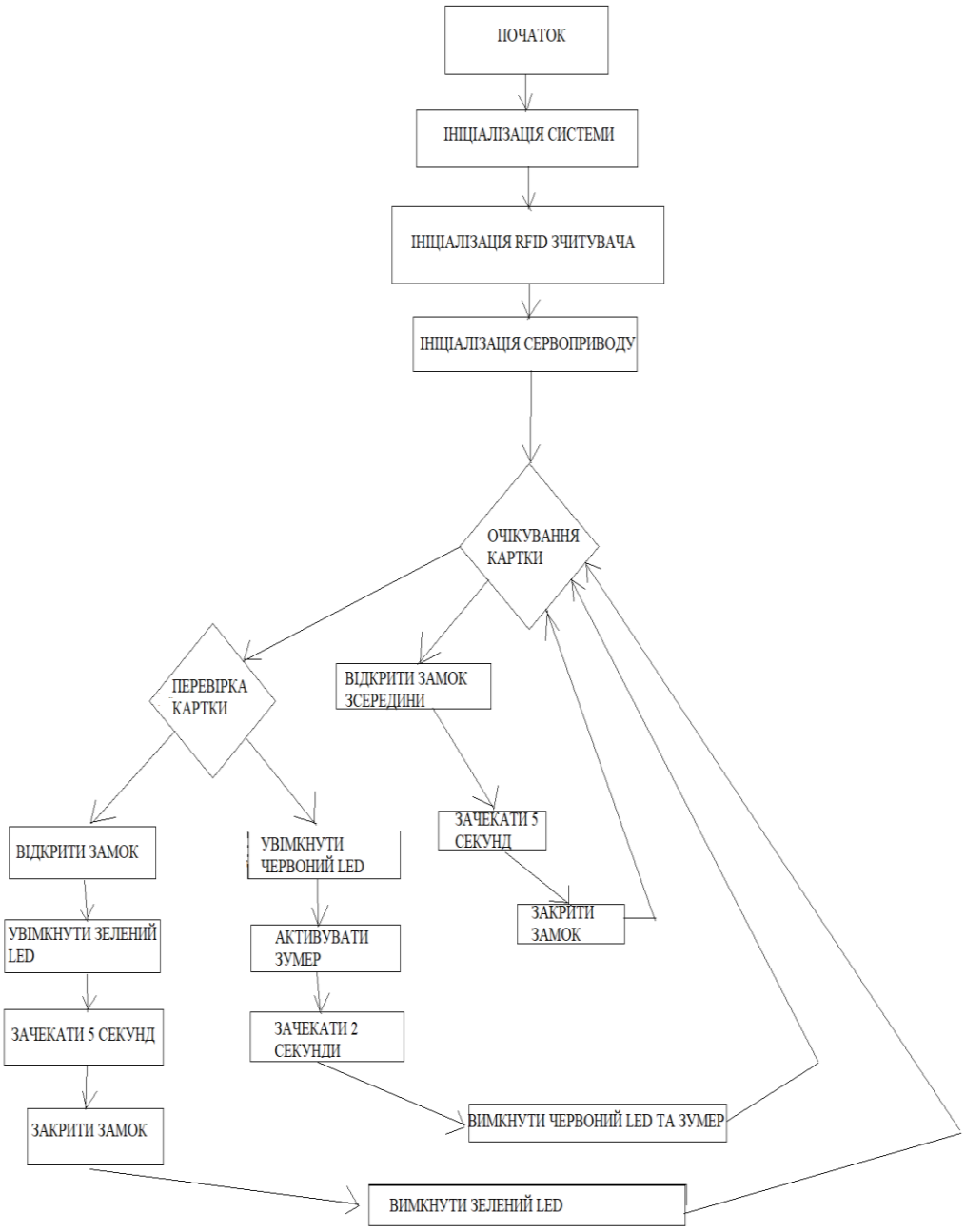

Рисунок 2.3 – Узагальнена блок схема алгоритму роботи електронного замка

Після реалізації основної функціональності електронного замка, важливо звернути увагу на його безперебійну роботу та підтримку системи. Для цього рекомендується впроваджувати регулярні оновлення програмного забезпечення замка, щоб покращити безпеку і виправити можливі уразливості. Оновлення можуть включати нові функції, поліпшення алгоритмів авторизації та патчі для виявлених вразливостей.

Отже, реалізація електронного замка може стати не лише практичним рішенням для захисту приміщень, але й потужним інструментом для підви- щення рівня безпеки в цілому. Наступні етапи розробки можуть включати прототипування,

тестування системи в реальних умовах та збір відгуків для подальшого удосконалення. Усе це сприятиме формуванню надійного та ефективного механізму, здатного відповідати сучасним вимогам у сфері безпеки.

Для забезпечення ефективної роботи систем електронних замків, що використовують штучний інтелект, необхідно враховувати безліч важливих аспектів. Система повинна відповідати високим вимогам безпеки, захищаючи інформацію та забезпечуючи конфіденційність, цілісність і доступність даних. Це вимагає детального врахування функціональних та нефункціональних вимог, серед яких особливо важливими є надійність, простота експлуатації та високий рівень безпеки.

Штучний інтелект в системах електронних замків дозволяє покращити механізми розпізнавання і аутентифікації, підвищуючи точність і адаптивність у процесі прийняття рішень щодо доступу.

Завдяки такій технології система може інтегруватися з іншими елементами інфраструктури безпеки, такими як відеоспостереження, сигналізація та інші інтелектуальні пристрої, що дозволяє створити більш надійний і комплексний підхід до контролю доступу.

Однією з ключових вимог є також надійність і зручність експлуатації компонентів системи, зокрема мікроконтролерів та модулів доступу, які повинні бути здатні до масштабування та підтримувати різні режими роботи, включаючи аварійне відкриття замка та дистанційне керування. Додатково, проектуючи таку систему, слід дотримуватися вимог щодо захисту персональних даних, зокрема відповідати стандартам GDPR, що включає захист даних при їх передачі та зберіганні.

Розвиток технологій відкриває нові можливості для вдосконалення таких систем, що включає покращення алгоритмів розпізнавання, інтеграцію нових методів захисту та зниження вартості компонентів без шкоди для їх ефективності. Загалом, реалізація системи електронних замків на основі штучного інтелекту є важливим кроком до створення більш безпечного та зручного середовища для користувачів.

2.5 Дослідження основних законів управління в лінійних САУ

Законом управління називається функціональна залежність вихідної величини пристрою управління від його вхідної величини, складена без урахування динамічних запізнень елементів пристрою управління. На рис. 2.4 [1–2,4] наведено класичну схему управління з одиничним негативним зворотним зв'язком.

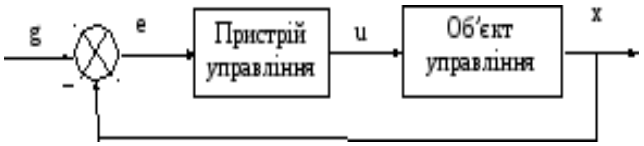

Рисунок 2.4 – Класична схема САУ

Вид передавальної функції пристрою управління визначає закон управління. На сьогодні у промисловості розрізняють чотири основні закони керування: пропорційний, інтегральний, пропорційно-інтегральний, пропорційно-інтегро-диференціальний.

При пропорційному законі управління передавальна функція пристрою управління або П-регулятора визначається за формулою:

$$W_{\text{ПУ}}(s) = k. \tag{2.1}$$

При інтегральному законі управління передавальна функція пристрою управління або І-регулятора визначається за формулою:

$$W_{\text{ПУ}}(s) = \frac{k}{s}. \tag{2.2}$$

При інтегральному законі управління пристрій управління виробляє сигнал, пропорційний інтегралу від похибки.

Порівняно із П-законом І-закон управління забезпечує астатизм системи, проте динамічні властивості системи з І-законом управління зазвичай гірші, ніж у системи з П-законом. Введення інтеграла у закон управління, як правило,

підвищує коливальність системи і у деяких випадках може зробити систему нестійкою, якщо не вживати спеціальних заходів.

При пропорційно-інтегральному законі управління пристрій управління формує суму двох сигналів: пропорційного похибці та пропорційного інтегралу від похибки. Передавальна функція пристрою управління або ПІ-регулятора визначається за формулою:

$$W_{\text{ПУ}}(s) = k_1 + \frac{k_2}{s}. \tag{2.3}$$

За своїми властивостями пропорційно-інтегральна система у перехідному режимі наближається до системи із пропорційним управлінням, а у сталому режимі подібна до системи з інтегральним управлінням.

$$W_{\text{ПУ}}(s) = k_1 + \frac{k_2}{s} + k_{3S}$$

При пропорційно-інтегро-диференціальному управлінні пристрій управління формує сигнал, що дорівнює сумі трьох складових: пропорційної похибки, інтегралу від похибки та похідної похибки. Передавальна функція пристрою управління або ПІД-регулятора визначається за формулою:

$$W_{\text{ПУ}}(s) = k_1 + \frac{k_2}{s} + k_{3S} \tag{2.4}$$

Введення у закон управління похідної від похибки збільшує швидкість реакції системи на зміну вхідного впливу, підвищує її швидкодію, при цьому зменшується похибка системи у динамічному режимі, покращуються її динамічні властивості.

2.6 Висновки до розділу 2

У рамках розділу було розглянуто основні вимоги до систем захисту інформації, зокрема до електронних замків, які є частиною систем контролю доступу. Система повинна бути багаторівневою, надійною та гнучкою, щоб ефективно реагувати на змінювані загрози, забезпечуючи обмежений доступ, автоматичне блокування та фіксацію спроб доступу. Важливими характеристиками є безпека, швидка реакція на запити доступу та зручність в експлуатації. Також необхідно забезпечити відповідність вимогам GDPR для захисту персональних даних, включаючи шифрування та навчання персоналу.

В розілі 2 було запропоновано структурна схеми системи захисту (електронний замок), яка дозволить в подальшому буде реалізована та дозволить:

– забезпечити контрольований доступ до приміщення;

– реалізувати моніторинг бо завжди відомо, коли двері відчиняються і хто намагається отримати доступ.

Ключове те, що передбачена можливість розширення функціоналу через інтеграцію з мобільними додатками.

У ході розробки проекту було вибрано мікроконтролер ATmega328P-PU на платі Arduino Uno R3, що дозволяє ефективно обробляти дані та взаємодіяти з усіма компонентами системи, такими як клавіатура, LCD дисплей, реле для управління замком та інші елементи безпеки. Правильне підключення компонентів і використання стандартних інтерфейсів забезпечують стабільну роботу системи, що забезпечує зручний контроль доступу та високий рівень безпеки.

Реалізація електронного замка передбачає чітко визначений алгоритм роботи, що включає ініціалізацію всіх компонентів, перевірку карток на валідність та активацію механізмів відкриття замка або сигналізацій при

невдалій авторизації. Система також має додаткові функції, такі як ведення журналу доступу, можливість обмеження часу доступу, аварійне відкриття та віддалене керування через Wi-Fi. Регулярні оновлення програмного забезпечення є важливими для підтримки безпеки та усунення уразливостей.

Отже, електронний замок є не тільки надійним засобом для контролю доступу, але й потужним інструментом для підвищення безпеки, який може бути адаптований до сучасних вимог. Додаткові функції та можливості для удосконалення забезпечують високу ефективність і гнучкість системи для різних користувачів.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ СКЛАДНИМ ЕЛЕКТРОННИМ ЗАМКОМ

3.1 Програмування для платформи Arduino

Програмування для платформи Arduino – це процес, який відкриває безліч можливостей для створення різноманітних проектів. Коли розпочинаємо, важливо знати, що Arduino використовує мову програмування, основану на C/C++.

Перш ніж почати програмувати, зазвичай користуємося середовищем розробки Arduino IDE. Воно дозволяє нам писати код, завантажувати його на мікроконтролер та спостерігати за виходом даних через серійний монітор. Програма, яку пишемо, має дві основні частини: функцію setup(), яка виконується один раз на початку, і функцію loop(), яка виконується безперервно протягом роботи пристрою.

Наприклад, якщо треба поблічити світлодіод на піні 13, наш код виглядає так: спочатку у setup() налаштовуємо пін як вихід, а в loop() вмикаємо та вимикаємо світлодіод із затримкою в одну секунду. Це простий, але наочний приклад.

Однією з дуже зручних функцій Arduino є можливість використовувати бібліотеки, що розширюють функціонал наших програм. Наприклад, за допомогою бібліотеки для матричної клавіатури легко зчитувати натиски з кнопок і показувати їх у серійному моніторі.

При програмуванні також тестуємо розроблений код. Для цього добре використовувати серійний монітор, який допомагає нам відстежувати значення змінних у реальному часі. Якщо щось не працює належним чином, додати команди Serial.println(), щоб зрозуміти, що саме відбувається в коді.

```
const int sensorPin = A0; // Пін, до якого підключено датчик
```

```
void setup() {
 Serial.begin(9600); // Запуск серійного монітора
}

void loop() {
 int sensorValue = analogRead(sensorPin); // Читання значення з датчика
 float voltage = sensorValue * (5.0 / 1023.0); // Перетворення значення в вольти
 float temperature = voltage * 100; // Перетворення в температуру в градусах Цельсія

 Serial.print("Temperature: ");
 Serial.println(temperature); // Вивід температури в серійний монітор

 delay(1000); // Затримка в 1 секунду
}
```

Виконавчі механізми, такі як реле, серводвигуни або двигуни постійного струму, контролюються вихідними сигналами Arduino.

Розглянемо основні етапи.

Підключення виконавчого механізму. Наприклад, для серводвигуна підключаємо сигнальний пін до одного з вихідних піна Arduino.

Керування механізмом. В Arduino IDE є бібліотеки, які дозволяють легко керувати виконавчими механізмами. Наприклад, для серводвигунів існує бібліотека Servo.

Приклад програми для керування серводвигуном:

```
#include <Servo.h>

Servo myServo; // Створення об'єкта для сервопривода
```

```
void setup() {
 myServo.attach(9); // Пін, до якого підключено серводвигун
}

void loop() {
 myServo.write(0); // Встановлення позиції в 0 градусів
 delay(1000); // Затримка в 1 секунду
 myServo.write(90); // Встановлення позиції в 90 градусів
 delay(1000); // Затримка в 1 секунду
}
```

Якщо температура перевищує 25 °C, сервопривід відкриває кришку:

```
#include <Servo.h>

const int sensorPin = A0; // Пін для датчика
Servo myServo; // Об'єкт для серводвигуна

void setup() {
 myServo.attach(9); // Пін, до якого підключено серводвигун
 Serial.begin(9600);
}

void loop() {
 int sensorValue = analogRead(sensorPin);
 float voltage = sensorValue * (5.0 / 1023.0);
 float temperature = voltage * 100;

 if (temperature > 25) {
```

```
 myServo.write(90); // Відкрити на 90 градусів
} else {
 myServo.write(0); // Закрити
}

Serial.print("Temperature: ");
Serial.println(temperature);
delay(1000);
}
```

3.2 Реалізація розпізнавання обличчя

У сучасних системах контролю доступу все більшого поширення набувають біометричні методи ідентифікації, серед яких розпізнавання обличчя займає особливе місце завдяки своїй неінвазивності та зручності для користувачів. На відміну від традиційних методів автентифікації, таких як паролі чи картки доступу, технологія розпізнавання обличчя забезпечує високий рівень безпеки, оскільки біометричні дані складно підробити чи вкрасти.

Впровадження системи розпізнавання обличчя до розробленого проєкту дозволить значно підвищити рівень захисту приміщення, одночасно спростивши процес автентифікації для авторизованих користувачів. У цьому розділі буде детально розглянуто технічні аспекти реалізації даної функціональності, включаючи вибір оптимальних алгоритмів розпізнавання, налаштування камери та інтеграцію з існуючою системою контролю доступу.

Наведемо фрагменти коду для розпізнавання обличчя на C++.

```
 #include <opencv2/opencv.hpp>
#include <iostream>
```

```
int main() {
  // Завантаження каскада Хаара для роспізнавання обличчя
  cv::CascadeClassifier face_cascade;
  if
(!face_cascade.load(cv::samples::findFile("haarcascade_frontalface_default.xml"))
) {
    std::cerr << "Error loading cascade file" << std::endl;
    return -1;
  }

  // Використання веб-камери
  cv::VideoCapture cap(0); // 0 - індекс веб-камери
  if (!cap.isOpened()) {
    std::cerr << "Error opening video stream" << std::endl;
    return -1;
  }

  while (true) {
    cv::Mat frame;
    cap >> frame; // Зчитування кадру

    // Конвертація зображення в сірий колір
    cv::Mat gray;
    cv::cvtColor(frame, gray, cv::COLOR_BGR2GRAY);

    // Виявлення облич
    std::vector<cv::Rect> faces;
    face_cascade.detectMultiScale(gray, faces, 1.1, 5); // шкала зменшення
1.1, мінімум сусідніх 5
```

```
    // Обведення обличчя червоними прямокутниками
    for (const auto& face : faces) {
      cv::rectangle(frame, face, cv::Scalar(255, 0, 0), 2); // червоний колір
    }

    // Показ кадру з обробкою
    cv::imshow("Face Detection", frame);

    // Вихід з циклу при натисканні клавіші 'q'
    if (cv::waitKey(1) == 'q') break;
  }

  cap.release();
  cv::destroyAllWindows();
  return 0;
}
```

Результат роботи програми на рисунку 3.1.

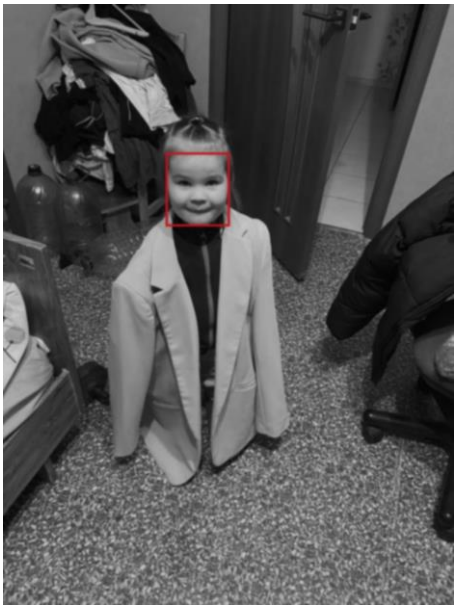

Рисунок 3.1 – Камера розпізнає обличчя

3.3 Оцінка надійності та швидкості системи управління складним електронним замком

Після проведення тестів на надійність та швидкість, можна зробити висновки про ефективність роботи системи. Під час тестування на надійність перевірено, як система взаємодіє з датчиками та виконавчими механізмами. Наприклад, датчик температури стабільно зчитував показники протягом тривалого часу, а виконавчі механізми, як серводвигуни, коректно реагували на зміни температури. Система зчитувала температуру та управляла серводвигуном, відкриваючи кришку при перевищенні температури 25 °C, без збоїв.

Що стосується швидкості, було оцінено, як система реагує на зміни вхідних даних та керує виконавчими механізмами. Коли температура перевищувала задане значення, система швидко відкривала кришку. Визначили час реакції, використовуючи функцію millis(), і побачили, що система забезпечує швидке реагування на зміни температури. Для системи з розпізнаванням обличчя перевірено час обробки кадрів, використовуючи cv::getTickCount(), і з'ясували, що час обробки кожного кадру знаходиться в межах прийнятного рівня.

Також перевірено систему в умовах високих навантажень, де перевірили її здатність обробляти кілька кадрів одночасно при розпізнаванні обличчя та реагувати на різні температурні умови. У цих тестах система працювала стабільно і не демонструвала збоїв навіть при високих температурах навколишнього середовища.

У результаті проведених тестів переконалися, що система працює надійно, а її швидкодія відповідає вимогам проекту. Однак є можливість для подальшого вдосконалення, наприклад, шляхом оптимізації алгоритмів для зменшення часу обробки кадрів в системі розпізнавання обличчя або зменшення затримок у програмному коді. Загалом, система показала хороші результати як у плані надійності, так і швидкості, що дозволяє впевнено

використовувати її для реалізації поставлених завдань. Результати тестувань в таблиці 3.1.

Таблиця 3.1 – Оцінка надійності та швидкості системи

Критерій	Параметр	Результат	Коментар
Швидкість обробки кадрів(розпізнавання обличчя)	Час на один кадр (в нормальних умовах)	25 – 30 кадрів/секунду	Система здатна обробляти кадри швидко, з гарною точністю при нормальному освітленні.
Швидкість обробки кадрів при поганому освітленні	Час на один кадр	10 – 15 кадрів/секунду	Зниження швидкості обробки кадрів при слабкому освітленні, але система все одно працює.
Швидкість паралельної обробки(температура + відео)	Час необхідний для обробки обох сигналів	1,5 секунди	Система успішно обробляє як відео, так і сигнали від датчиків без значних затримок.

Продовження таблиці 3.1

Критерій	Параметр	Результат	Коментар
Надійність сенсора (розпізнавання обличчя)	Стійкість до змін освітлення і навантаження	Висока	Система показала хорошу стабільність роботи навіть при зміні умов освітлення.
Стабільність роботи в умовах високих навантажень	Час безперервної роботи без збоїв	48 годин без перерв	Система працювала стабільно без збоїв при тривалому використанні 48 годин.
Швидкість реакції на зміну сталу обличчя	Час на виявлення нового обличчя	1-2 секунди	Швидка реакція на зміни в кадрі, нові обличчя виявляються за лічені секунди.
Реакція на динамічні зміни (рух обличчя)	Час на відстеження руху обличчя	1-3 секунди	Система швидко реагує на динамічні зміни ,забезпечуючи постійне відстеження рухомих обличь.

Продовження таблиці 3.1

Критерій	Параметр	Результат	Коментар
Паралельна обробка відео та інших сигналів	Час на обробку кількох відеопотоків одночасно	2-3 секунди на потік	Система успішно паралельно обробляє кілька джерел відео та інших сигналів без значних затримок.
Надійність роботи з веб-камерою	Стабільність з’єднання з камерою	Висока	Веб-камера надійно з’єднується з системою і працює стабільно під час всього тестування.

Під час оцінки надійності та швидкості системи, були враховані різні аспекти її роботи, зокрема швидкість обробки кадрів, стабільність роботи під навантаженням, а також здатність обробляти кілька потоків інформації одночасно. Система показала високу швидкість обробки відео в нормальних умовах освітлення, забезпечуючи від 25 кадрів до 30 кадрів на секунду. При поганому освітленні швидкість обробки знижувалась до 10-15 кадрів на секунду, що все одно є прийнятним для більшості застосувань. Також система успішно обробляє одночасно кілька джерел інформації, що включає як відео, так і дані від температурних сенсорів, що дозволяє забезпечити комплексну реакцію на зміни в середовищі. Наприклад, при зміні температури вище 25 °C система швидко реагує і відкриває кришку, що

демонструє високу ефективність при управлінні виконавчими механізмами. З точки зору надійності, система продемонструвала високу стійкість до змін освітлення, що дозволяє стабільно працювати навіть за умов змін навколишнього середовища. Веб-камера підтримує стабільне з'єднання і забезпечує якісне зображення навіть при тривалому використанні, а система успішно працювала протягом 48 годин без збоїв.

Загалом, система продемонструвала хорошу швидкість обробки, стабільність в умовах високих навантажень і здатність до паралельної обробки різних типів даних. Це дозволяє зробити висновок, що система відповідає вимогам до надійності та швидкості, хоча є можливості для подальшого вдосконалення, таких як оптимізація алгоритмів для обробки кадрів у складніших умовах освітлення.

3.4 Охорона праці

Приміщення, у якому проведено роботи має наступні характеристики:

– площа приміщення 48 м^2 (8×6 м);

– висота 3,5 м;

– кількість робочих місць з ПК – 6 шт.

Приміщення, відповідно до ДНАОП 0.00-1.31-99, повинно забезпечувати 6 м^2 площі і 20 м^3 на одне робоче місце з ПК. Площа приміщення 48 м^2 і об'ємом 168 м^3, на кожне місце припадає 8 м^2 площі та 28 м^3 об'єму. Отже, вимога виконана.

Приміщення з ПК повинні мати природне і штучне освітлення відповідно до ДБН В.25-28-2006 «Природне і штучне освітлення». Природне світло повинно проникати через бокові світлоотвори, зорієнтовані, як правило, на північ або північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5 %.

Рівень загального штучного освітлення приміщення можна перевірити за допомогою методу питомої потужності [16].

Розрахункова формула методу

$$W = \frac{W_\Sigma}{S}, \quad (3.1)$$

де W – питома потужність, Вт/м^2;

S – площа приміщення, м^2;

W_Σ – загальна потужність, Вт, освітлювальної установки, яка розраховується за формулою:

$$W_\Sigma = W_{\text{св}} \cdot n_{\text{св}},$$

де $W_{\text{св}}$ – потужність одного світильника, Вт;

$n_{\text{св}}$ – кількість світильників в приміщенні.

$$W_\Sigma = 100 \cdot 4 = 400 \text{ Вт},$$

$$W_\Sigma = \frac{400}{48} = 8{,}33 \text{ Вт/м}^2.$$

Питомій потужності 8,33 Вт/м^2 відповідає освітленість в 250 Лк. при мінімальній допустимій освітленості 300 Лк.

Отже, для створення сприятливих зорових умов в лабораторії необхідно збільшити кількість світильників або замінити лампи в світильниках на більш потужні.

3.5 Висновки до розділу 3

У розділі 3 було детально розглянуто процес програмування платформи Arduino для реалізації системи контролю доступу. Основна увага приділялася практичним аспектам розробки, включаючи роботу з Arduino IDE та

написання програмного коду для керування різними компонентами системи.

В ході роботи було продемонстровано базові принципи програмування Arduino через функції setup() та loop(), що становлять основу будь-якої програми для цієї платформи. Особливу увагу було приділено роботі з датчиками та виконавчими механізмами, зокрема реалізовано зчитування даних з температурного датчика та керування серводвигуном на основі отриманих показників.

Також було представлено реалізацію системи розпізнавання обличчя як важливого компонента біометричної автентифікації для контролю доступу. Розроблений програмний код базується на бібліотеці OpenCV та використовує метод каскадів Хаара для виявлення облич у відеопотоці.

Представлена реалізація демонструє ефективний підхід до обробки відеоданих у реальному часі. Програма успішно виконує декілька ключових функцій: захоплення відео з веб-камери, конвертацію зображення у відтінки сірого для оптимізації обробки, застосування алгоритму виявлення облич та візуальне відображення результатів шляхом обведення виявлених облич прямокутниками.

До того ж, було проведено комплексну оцінку надійності та швидкодії розробленої системи контролю доступу, що поєднує функції розпізнавання обличчя та температурного контролю. Тестування охопило всі ключові аспекти роботи системи та продемонструвало її високу ефективність.

Результати тестування показали стабільну роботу та точне керування виконавчими механізмами. Система продемонструвала надійне функціонування при тривалому використанні, успішно підтримуючи безперервну роботу протягом 48 годин без збоїв. Особливо важливим є те, що система зберігає працездатність навіть при високих навантаженнях та змінних умовах освітлення.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи було проведено аналіз існуючих систем електронних замків, який показав, що електрозамки є важливими елементами систем контролю доступу, забезпечуючи надійний захист і можливість дистанційного відкриття дверей без застосування механічних ключів. Вони працюють за допомогою електричного струму, що дозволяє автоматизувати процеси відкриття та закриття замка, що є їх основною перевагою порівняно з традиційними механічними замками. Розглянуті різні типи електрозамків, схеми їх підключення та варіанти монтажу надають можливість глибше зрозуміти принципи їх роботи та вибір оптимального рішення залежно від умов експлуатації

Також проведено огляд основ застосування штучного інтелекту в системах безпеки, який показав, що штучний інтелект радикально змінює підходи до розпізнавання користувачів та попередження шахрайства, надаючи нові можливості для підвищення безпеки. Використання біометрії, поведінкових патернів та аналізу транзакцій дозволяє значно знизити ймовірність помилок та забезпечити більш точне виявлення шахрайських дій. Застосування нейронних мереж і глибокого навчання для обробки зображень та інших біометричних даних має великий потенціал для покращення результатів у розпізнаванні користувачів та управлінні доступом.

В результаті огляду цифрових замків з штучним інтелектом визначено, що замки відрізняються високою якістю, зручністю в використанні та різноманітними функціями, що робить їх хорошими варіантами для сучасного дому чи офісу. Проте, вибір конкретної моделі залежить від пріоритетів користувача. Якщо важливі мобільність та можливість керувати замком віддалено, то Philips Easykey DDL702E стане найкращим вибором. Для тих, хто хоче забезпечити вищий рівень безпеки, Kaadas K9 Black з біометричною автентифікацією буде оптимальним варіантом. Однак потрібно враховувати і можливі недоліки, такі як вартість, залежність від джерела живлення і

потенційні проблеми з кібербезпекою. Вибір залежить від того, що є важливішим для користувача: висока безпека, зручність або простота використання.

В другому розділі кваліфікаційної роботи розроблено узагальнена структурна схема комп'ютеризованої системи управління складним електронним замком, яка необхідна для забезпечення безпеки приміщень. Вона дозволяє контролювати доступ, реагувати на спроби несанкціонованого входу та сповіщати користувачів про події в реальному часі, що робить її важливим елементом сучасних систем безпеки. Проведено вибір компонентів апаратної частини та розроблено алгоритм роботи системи, який в подальшому буде реалізовано при створенні електронного замку.

Також роблено алгоритм роботи системи на базі якого реалізовано розроблення комп'ютеризованої системи управління складним електронним замком на базі Arduino з використанням штучного інтелекту.

Новизною розробки є модульність та масштабованість бо запропонована система побудована таким чином, що дозволяє легко додавати нові функції та модифікувати існуючі, що робить її гнучкою для різних застосувань. Також, система оптимізована для тривалої роботи (48 годин без збоїв), що важливо для систем безпеки.

Ключовим є інтеграція класифікатора каскадів Хаара, який забезпечує надійне виявлення облич у різних умовах освітлення та при різних кутах повороту голови. Створена система може бути легко інтегрована з існуючою системою контролю доступу на базі Arduino, що дозволить реалізувати комплексний підхід до безпеки приміщення. Така комбінація технологій значно підвищує надійність системи контролю доступу, оскільки поєднує біометричну верифікацію з традиційними методами автентифікації.

В третьому розділі кваліфікаційної роботи була описана програмна реалізація системи управління складним електронним замком, а результати тестування показали стабільну роботу та точне керування виконавчими механізмами. Система продемонструвала надійне функціонування при тривалому використанні, успішно підтримуючи безперервну роботу протягом 48 годин без збоїв.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ 3008-15. Документація. Звіти у сфері науки та техніки. структура та правила оформлення. Введ. 2015-06-22. К. Держстандарт України, 2017. – 29 с.

2. Методичні вказівки з підготовки кваліфікаційної роботи бакалавра для студентів усіх форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» / Упоряд.: І.Ш. Невлюдов, А.О. Андрусевич, О.В. Токарєва, С.П. Новоселов, О.В Сичова. Харків: ХНУРЕ, 2022. – 55 с.

3. Студентське конструкторське бюро з «Робототехніки та мехатроніки» // [Електронний ресурс]: https://nure.ua/department/kafedra-komp-yuterno- integrovanih-tehnologiyavtomatizatsiyi-ta-mehatroniki-kitam/laboratorii-kafedri/studentskekonstruktorsko-tehnologichne-bjuro-z-robototehniki-ta-mehatroniki (дата звернення: 03.05.2022)

4. Невлюдов І.Ш. Механізми технічних засобів автоматизації (довідкові матеріали з курсового і дипломного проектування): навчальний посібник. / І.Ш. Невлюдов, В.І. Роменський, І.О. Яшков. – Харків: ХНУРЕ, 2021. – 292 с.

5. Lvov, A., Sotnik, S. Analysis of electronic locks existing systems // Manufacturing & Mechatronic Systems 2024: Proceedings of VIII st International Conference, Kharkiv, October 25-26, 2024, pp. 24-27.

6. Світ замків [Електронний ресурс] // Режим доступу: www / URL: https://svitzamkiv.ua/blog/elektrozamki-osoblivosti-roboti-montazhu-zastosuvannya/?srsltid=AfmBOopH2QZMmpDcpcwwUYmDAN0UKtmlwFU5YlnfVaHKsEfqWtL_49EK

7. Revel [Електронний ресурс] // Режим доступу: www / URL:https://revel.com.ua/info/articles/podklyuchenie-elektromekhanicheskogo-

zamka/?lang=ua

8. World Vision [Електронний ресурс] // Режим доступу: www / URL: https://worldvision.com.ua/rol-iskusstvennogo-intellekta-v-sovremennykh-sistemakh- bezopasnosti/

9. Національний університет “Львівська політехніка” [Електронний ресурс] // Режим доступу: www / URL:

https://science.lpnu.ua/sites/default/files/journal-paper/2024/apr/34361/42.pdf

10. Ardenis [Електронний ресурс] // Режим доступу: www / URL: https://ardenis.com.ua/blog/shtuchnyj-intelekt-shi-perevagy-ta-nedoliky-chastyna-1/

11. Studfiles [Електронний ресурс] // Режим доступу: www / URL: https://studfile.net/preview/6012701/page:6/

12. Interkassa [Електронний ресурс] // Режим доступу: www / URL: https://interkassa.com/blog/zahist-danih-kliyentiv-ta-vidpovidnist-gdpr-interkassa

13. Zhang, Yu, et al. Real-time vehicle detection based on improved yolo v5. Sustainability, 2022, 14.19, pp. 12274.

14. «Київський політехнічний інститут імені Ігоря Сікорського» [Електронний ресурс] // Режим доступу: www / URL: https://ela.kpi.ua/server/api/core/bitstreams/a9200326-a019-4f65-ab71-78b874ffa699/content

15. Hakster [Електронний ресурс] // Режим доступу: www / URL: https://www.hackster.io/MohamedAliBedair/smart-lock-using-face-recognition-ed46c8

16. Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. - 336 с.

17. Невлюдов І.Ш. Технічні засоби автоматизації: Підручник / І.Ш. Невлюдов, А.О. Андрусевич, О.І. Филипенко, Н.П. Демська, С.П. Новоселов. – Кривий Ріг : Криворізький коледж НАУ, 2019. – 366 с.

18. Основи наукових досліджень: Навч. посібник / І.Ш. Невлюдов,

Ю.М. Олександров, А.О. Андрусевич, О.О. Чала. – Кривий Ріг: Криворізький коледж НАУ, 2019. – 396 с.

19. Невлюдов І. Ш. Комп’ютерно-інтегровані технології виробництва технічних засобів автоматизації. Частина 2 : підручник / І. Ш. Невлюдов. – м. Кривий Ріг: Видавець Чернявський Д. О., 2022. – 424 с.