Міністерство освіти і науки України
Одеський національний технологічний університет
Кафедра комп'ютерної інженерії

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему *Розробка системи управління доступом до квартири*
(назва кваліфікаційної роботи згідно наказу ОНТУ)

Здобувача *Адаховської Ю.В.*
(прізвище, ініціали)

3 скор. курсу *757с3* групи

Керівники: *ст. викл. Жирнова Т.М.*
(посада, прізвище та ініціали)

д.т.н, проф. Артеменко С.В.
(посада, прізвище та ініціали)

Консультанти *д.е.н., проф. Басюркіна Н.Й.*
(посада, прізвище та ініціали)

ст. викл. Жуковецька С.Л.
(посада, прізвище та ініціали)

Кваліфікаційна робота допускається до захисту

Рішення кафедри від *10.06* *2023* р., протокол № 8

Завідувач кафедри комп. інженерії _____ Сергій АРТЕМЕНКО
(назва кафедри) (підпис) (Ім'я ПРІЗВИЩЕ)

Одеса - 2023 рік

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерної інженерії, програмування та кіберзахисту*
Кафедра *комп'ютерної інженерії*
Ступінь вищої освіти *бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*
Освітня програма *Мережеві технології та інтернет речей*

ЗАТВЕРДЖУЮ
Зав. кафедри *комп'ютерної інженерії*
Сергій АРТЕМЕНКО
« 10 » *серпня* 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Адаховської Юлії Валеріївни

1. Тема роботи *Розробка системи управління доступом до квартири*

Затверджена наказом університету від « *10* » *серпня* *2022* р., наказ № *440-03*

2 Термін здачі здобувачем закінченої роботи *5 червня 2023 р.*

3. Вихідні дані роботи

сфери використання систем управління доступом, вимоги до систем управління доступом, апаратні платформи для проектування систем управління, протоколи управління «розумним будинком», Редактор MS Power Point

4. Перелік питань, які потрібно розробити

1. Вступ. 2. Збір та аналіз інформації. 3. Аналіз компонент та технологій систем контролю управління доступом. 4. Розробка системи управління. 5. Загальні висновки. 6. Економічні розрахунки. 7. Охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Презентація Power Point: Слайд 1. Мета, предмет, об'єкт. Слайд 2. Задачі. Слайд 3. Вимоги до систем управління доступом. Слайд 4. Технічне завдання. Слайд 5.Вибір електронних компонентів. Слайд 6. Структурна та функціональна схема пристрою. Слайд 7. Використане програмне забезпечення. Слайд 8. Економічні розрахунки. Слайд 9. Загальні висновки.

6. Консультанти по роботі, із зазначенням розділів роботи, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Економіка	*Басюркіна Н.Й., д.е.н., проф.*		
Охорона праці	*Жуковецька С.Л., ст.викл.*		
Нормоконтроль	*Жирнова Т.М., ст.викл.*		

7. Дата видачі завдання *30.09.2022*

Керівники _____ *Тетяна ЖИРНОВА*

_____ *Сергій АРТЕМЕНКО*

Завдання прийняв до виконання _____ *Юлія АДАХОВСЬКА*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Постановка завдання.*	*20.02.23*	
2.	*Визначення вхідних даних.*	*10.03.23*	
3.	*Аналіз систем контролю управління доступом*	*16.03.23*	
4.	*Аналіз платформ та технологій інтернету речей*	*20.03.23*	
5.	*Розробка системи контролю управління доступом*	*15.04.23*	
6.	*Економічні розрахунки.*	*15.04.23*	
7.	*Охорона праці*	*5.05.23*	
8.	*Оформлення розрахунково-пояснювальної записки*	*20.05.23*	
9.	*Підготовка графічного матеріалу*	*3.06.23*	

Керівники роботи _____ *Тетяна ЖИРНОВА*

_____ *Сергій АРТЕМЕНКО*

Несу відповідальність за ідентичність електронного та друкованого варіантів кваліфікаційної роботи, даю згоду на обробку персональних даних та не заперечую проти розміщення кваліфікаційної роботи на офіційних web-ресурсах ОНТУ.

Підтверджую, що в кваліфікаційній роботі відсутні порушення норм академічної доброчесності.

Здобувач - дипломник _____ *Юлія АДАХОВСЬКА*

АНОТАЦІЯ

У сучасному світі, в даний момент відбувається швидкий розвиток мобільних технологій. Техніка стає все більш універсальною, компактною, продуктивнішою. Паралельно розвиваються засоби бездротового зв'язку.

Система управління доступом – це сукупність апаратно-програмних засобів і організаційних заходів для захисту від несанкціонованого доступу.

Метою роботи є розробка моделі приладу системи управління доступом до квартири, яка дозволить досягти економічного ефекту, та матиме можливість модернізувати та удосконалювати систему.

Для вирішення поставленої мети у роботі розроблена система, що дозволяє користувачеві управляти режимом роботи електромеханічного замку, пристроями світлового та звукового оповіщення за допомогою смартфона або іншого електронного пристрою за допомогою зв'язку *Wi-Fi*. Для удосконалення безпеки у проекті перебачено безперебійне джерело живлення на сонячних батареях. Також проведено вибір електронних компонентів та розроблено функціональні схеми: підключення *Wi-Fi* модуля, підключення електромагнітного реле, підключення пристроїв світлового та звукового сповіщення, підключення сонячних модулів та блока живлення. Розроблено алгоритм управління для мікроконтролера *Arduino UNO*.

У роботі виконано підрахунок вартості всіх комплектуючих для створення пристрою, який довів економічну перевагу над існуючими рішеннями.

В рамках даної випускної кваліфікаційної роботи була показана актуальність розвитку систем контролю та управління доступом.

ABSTRACT

In today's world, there is a rapid development of mobile technologies. Technology is becoming more and more versatile, compact, and more productive. At the same time, wireless communications are developing.

An access control system is a set of hardware and software tools and organizational measures to protect against unauthorized access.

The aim of the work is to develop a model of the device for the access control system to the apartment, which will achieve an economic effect and will be able to modernize and improve the system.

To achieve these goals, a system has been developed in the work that allows the user to control the operating mode of an electromechanical lock, light and sound warning devices using a smartphone or other electronic device via a Wi-Fi connection. To improve safety, the project provides for an uninterruptible solar power supply. A selection of electronic components was made and functional diagrams were developed: connecting a Wi-Fi module, connecting an electromagnetic relay, connecting light and sound warning devices, connecting solar modules and a power supply. A control algorithm for the Arduino UNO microcontroller has been developed.

In the work, the cost of all components for creating the device was calculated, which proved the economic advantage over existing solutions.

As part of this final qualification work, the relevance of the development of access control and management systems was shown.

ЗМІСТ

					КРБ.КІ.1.440–03.6.1		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Юлія АДАХОВСЬКА			Розробка системи управління доступом до квартири	Літ.	Арк. 6 / Акрушів 84
Перевірив		Тетяна ЖИРНОВА					
Рецензент						гр. 757с3, ОНТУ	
Нормоконтроль		Тетяна ЖИРНОВА					
Затвердив		Сергій АРТЕМЕНКО					

ВСТУП

У сучасному світі, в даний момент відбувається швидкий розвиток мобільних технологій. Техніка стає все більш універсальною, компактною, продуктивнішою. Паралельно розвиваються засоби бездротового зв'язку, дозволяючи передавати дані швидше та надійніше. Розвиток технологій впливає на інші сфери, такі як сфера безпеки, даючи їй нові обладнання та зручності. У сфері безпеки, під мобільним доступом розуміють систему, в якій для отримання доступу до даних та інших ресурсів, як пристрій-ідентифікатор використовується мобільний пристрій.

СКУД – система контролю та управління доступом – це засіб захисту від неправомірного доступу сторонніх осіб на будь-яку територію (підприємство), розмежування рівня доступу співробітників у внутрішні приміщення. Також СКУД є ефективним засобом підвищення ефективності управління персоналом.

У широкому сенсі СКУД – це сукупність апаратно-програмних засобів і організаційних заходів. Її головне завдання – автоматизувати процес санкціонованого контрольованого доступу і обліку співробітників, відвідувачів і транспортних засобів на території підприємства.

Застосування систем контролю та управління доступом – це один із підходів для забезпечення безпеки окремо взятого об'єкта. Найбільш популярною сферою інтеграції СКУД з функцією моніторингу та управління є використання даної технології у розробці «розумного будинку». Технологія «розумний будинок» є складним комплексом різних технічних пристроїв, керованих єдиним центром для підтримки заданих параметрів, забезпечення комфорту та безпеки людей, що живуть у домі. Основними перевагами використання технологій «розумного будинку» є: економія ресурсів, ефективна експлуатація інженерних систем будинку, підвищення комфорту та безпеки.

Метою роботи є розробка моделі приладу системи управління доступом до квартири, яка дозволить досягти економічного ефекту, та матиме можливість модернізувати та удосконалювати систему.

Об'єктом дослідження є система, яка надає можливість ідентифікації та має можливість керувати санкціонованим доступом до об’єкту охорони.

Предметом дослідження є технології та інструменти створення система контролю та управління доступом.

Задача роботи полягає у виборі технології, а також розробці системи контролю управління доступом за допомогою бездротового зв’язку. Для систем управління необхідно вибрати технологію, засоби контролю та апаратні пристрої, розробити алгоритми управління.

Для досягнення поставленої задачі необхідно вирішити наступні завдання:

- вивчить відповідні тематиці джерела;
- оцінити актуальність систем контролю управління доступом;
- провести аналіз існуючих СКУД;
- провести аналіз апаратних платформ для реалізації пристрою, що проектується;
- розробити структурну та функціональну схему системи управління;
- обґрунтувати вибір контролера, комплектуючих та допоміжного обладнання;
- розробити алгоритми управління та програму для мікроконтролера.

РОЗДІЛ 1
ЗБІР ТА АНАЛІЗ ІНФОРМАЦІЇ

1.1 Актуальність систем контролю управління доступом

За даними дослідження компанією *Fact MR* (американська дослідницька компанія, що спеціалізується на дослідженні ринків), середньорічний темп зростання даного сегменту ринку систем безпеки досягне понад 8% протягом найближчих 10 років. Затребуваність технології систем контролю управління доступом для охорони комерційних та житлових будівель, як і раніше, залишатиметься на високому рівні. При цьому продажі в сегменті доступу за картами-зчитувачами перевищать 5 млрд. доларів до 2031 року. Проте біометричні технології демонструватимуть високі середньорічні темпи зростання глобального ринку електронних систем контролю доступу.

Впровадження електронних систем контролю доступу, як і раніше, зосереджено в комерційній галузі. За прогнозами аналітиків, виторг від реалізації проектів для приватного, у тому числі і промислового секторів, залишиться на високому рівні і до кінця 2023 року сягне понад 4,3 млрд. доларів. До кінця 2031 року державний та оборонний сектори у вартісному вираженні перевищать 6,6 млрд. доларів. Зростання впровадження електронних систем контролю доступу у галузі охорони здоров'я також стане одним із основних драйверів зростання.

Основним драйвером експерти вважають зростаючу потребу високого рівня безпеки в корпораціях. Збільшується попит на біометрію, смарт-картки, безконтактні рішення щодо ідентифікації користувача, а також, оскільки більшість корпоративних співробітників використовують свої мобільні пристрої для доступу до даних компанії, збільшується сегмент мобільних рішень для контролю, оскільки ці пристрої дуже вразливі для атак.

Зчитувачі на основі карток, як очікується, продовжать домінувати на ринку обладнання контролю доступу протягом прогнозованого періоду. Зростаюча потреба в смарт-картах та безконтактних картах для відстеження та запису дій співробітників є одним із факторів, що сприяють зростанню ринку зчитувачів.

Експерти прогнозують, що ринок біометричних зчитувачів розвиватиметься протягом прогнозованого періоду найвищими темпами. Біометричні технології використовуються для вимірювання різних фізіологічних параметрів для ідентифікації та аутентифікації в системах контролю доступу. Ринок систем контролю доступу на основі біометричних зчитувачів поділено на наступні категорії: розпізнавання відбитків пальців, розпізнавання долоні, розпізнавання райдужної оболонки ока, розпізнавання облич та розпізнавання голосу. Біометрія – одна з технологій, що найбільш швидко зростає у використанні для захисту периметра. Ця технологія дозволяє визначати фізичні характеристики людини забезпечення контрольованого фізичного доступу до інфраструктури. Ця технологія все частіше використовується на державних об'єктах, виробничих підприємствах, електростанціях та оборонних підприємствах.

Очікується також, що житлова вертикаль стане найшвидшим ринком контролю доступу протягом прогнозованого періоду. У житлових приміщеннях все частіше використовуються системи контролю доступу. У житлових будинках встановлюються системи контролю доступу для запобігання вторгненням та крадіжкам із зломом. Ці об'єкти дедалі частіше використовують системи контролю доступу з урахуванням електронних замків. Попит на електронну продукцію зростає разом із зростаючою тенденцією домашньої автоматизації. Ключові фактори, що сприяють зростанню цього ринку, включають зростаючий рівень злочинності, постійні технологічні досягнення, зростаючу потребу у виявленні небезпек, таких як пожежа та витік газу, а також забезпечення безпеки дітей та людей похилого віку.

Варто відзначити активне впровадження *IP* технологій у цю сферу. Вже понад 10 років використовуються локальні обчислювальні мережі передачі інформації у деяких системах контролю та управління доступом. У таких випадках часто використовуються інтерфейси *RS*-485 для об'єднання контролерів у загальну мережу по каналах *Ethernet*. З точки зору компонентів СКУД *Wi-Fi* канали можуть бути відмінною заміною проводового *Ethernet*, адже підключені до бездротових точок доступу пристрою не відрізнять одне середовище передачі від іншого. При цьому даний спосіб передачі даних дозволяє уникнути труднощів з здійсненням комунікації між компонентами системи, на відміну від використання стандартного інтерфейсу *RS*-485. У міру розвитку мереж *Wi-Fi* популярність такого способу комунікації в системах контролю та управління доступом буде тільки зростати, адже даний спосіб за фінансовими витратами помітно виграє у стандартних методів через відсутність необхідності прокладання проводового каналу зв'язку довжиною в кілька десятків метрів.

Чинниками, які прискорюють зростання ринку СКУД, є:

− зростаюча кількість терористичних атак та організованої злочинності в усьому світі;

− зростання впровадження систем безпеки на основі Інтернету речей з платформами хмарних обчислень;

− постійні технологічні досягнення та зростаюче розгортання бездротових систем безпеки;

− зростаюча поінформованість про домашні системи безпеки;

− впровадження управління доступом, як послуга (*Access Control as a Service або ACaaS* – контроль доступу як послуга);

− поступове впровадження управління доступом на основі мобільних пристроїв;

− швидка урбанізація в країнах, що розвиваються;

− глобальне поширення ініціатив розумних міст.

Основні висновки з дослідження ринку показують, що Азіатсько-Тихоокеанський регіон, за винятком Японії, як очікується, стане найбільшим на світовому ринку електронних рішень контролю доступу. Внаслідок цього очікується, що ця географічна область створить додаткові можливості на суму понад 310 мільйонів доларів протягом 2021-2031 років. Після цього ринок електронних систем контролю доступу в Північній Америці, ймовірно, стане другим за величиною ринком протягом прогнозованого періоду.

Варто зазначити, що ринок систем безпеки дуже консолідований, і виробники намагаються зберегти своє довгострокове домінування на ньому. Наприклад, ключові виробники постійно беруть участь у розробці нових продуктових лінійок, щоб вийти на нову арену застосувань. Більше того, їхня жага домінування на ринку висока через швидкозростаючу індустрію з більш високим потенціалом.

1.2 Аналіз систем контролю управління доступом

Усі сучасні системи контролю управління доступом можна розділити на мережні і автономні. Автономні системи є в найпростішому випадку кодонабірними панелями і використовуються в приватних котеджах і невеликих компаніях, що розміщуються в декількох кімнатах.

У разі мережевих СКУД всі контролери з'єднані один з одним і підключені до комп'ютера, забезпечуючи взаємопов'язану роботу окремих точок доступу до системи. У великих системах це дає масу переваг щодо контролю та організації складних механізмів проходу. Потужні мережеві СКУД із великими функціональними можливостями встановлюють на підприємствах, у банках.

Системи контролю доступу для розумного будинку включають:

− автономні – для керування одним або декількома пристроями, що перегороджують, без передачі інформації на центральний пульт або без контролю з боку оператора;

− централізовані (мережеві) – для регулювання пристроями, що перегороджують, з обміном інформацією з центральним пультом і контролем і керуванням системою з боку оператора. Призначені для забезпечення контролю та керування доступом на великих об'єктах. Виділяють чотири характерні типи точок доступу, де може бути застосований контроль: офісні приміщення (електромагнітні замки; зчитувачі дистанційного типу з великою відстанню зчитування, для того, щоб службовці не виймали картки з кишені – принцип вільних рук; електромагнітні клямки), об'єкти на вулиці (ворота, шлагбауми для автостоянок, система зчитування та розпізнавання автомобільних номерів і т.д.);

− універсальні, що включають функції як автономних, так і мережевих систем, що працюють в мережевому режимі під керівництвом центрального пристрою управління і переходять в автономний режим у разі відмов у мережевому обладнанні та центральному пристрої або при обриві зв'язку.

Алгоритм роботи точки доступу, що захищається системою, залежить насамперед від самої точки доступу.

Двері – найпоширеніший спосіб доступу до приміщення. Пристрій для замикання дверей підбирається залежно від конфігурації, напряму відкривання, матеріалу. Пристроєм може бути електромеханічний або електромагнітний керований замок або клямка. Правильно встановлені двері – гарна перешкода для несанкціонованого доступу до приміщення. Недолік, про який потрібно пам'ятати при організації роботи системи, полягає в тому, що слідом за особою, яка має доступ і відкрила двері в приміщення, що захищається, може пройти інша людина.

Турнікети зустрічаються головним чином в об'єктах з великою кількістю співробітників. На відміну від дверей, при правильному налаштуванні системи, вони дозволяють пропускати лише одну людину. Це, а також висока пропускна спроможність робить їх незамінними на прохідних підприємств та офісних центрів.

Шлагбаумами та воротами обладнуються в'їзди на території підприємств та закритих автомобільних стоянок. З точки зору СКУД за логікою доступу вони подібні до дверей. Завдання автоматичної ідентифікації не тільки людини, що в'їжджає на об'єкт, а й автотранспорту, що успішно реалізується завдяки зчитувачам великої дальності, здатним з декількох метрів розпізнавати мітки, що прикріплені до автомобіля.

Шлюзові кабіни використовуються там, де до безпеки пред'являються особливі вимоги. Не всі СКУД здатні обслуговувати такі складні пристрої, що обмежує їхню реалізацію. За пристроєм це можуть бути дві послідовно розташовані двері, так що в конкретний момент часу відкрита тільки одна. Більш складний варіант роботи шлюзу: в кабіні, крім датчика присутності, знаходиться вагова платформа, і доступ в приміщення відкривається, коли вага вхідної людини «збігається» із зазначеним для неї в базі даних.

Розглянемо тепер поширені алгоритми доступу, можливі завдяки інтелектуальної складової системи. До неї входять контролери, пристрої ідентифікації (*proximity*-зчитувачі, зчитувачі смарт-карток, біометричні зчитувачі), ідентифікатори та програмне забезпечення, під керуванням якого працює система.

Наведені далі алгоритми, переважно, застосовні для мережевих СКУД, так як для їх реалізації необхідна злагоджена робота окремих точок доступу і можливість управління від комп'ютера.

Найпростіший спосіб ідентифікації на точці проходу – набір ПІН-коду на клавіатурі зчитувача. З одного боку, при цьому у людини не повинно бути будь-яких зовнішніх ідентифікаторів, з іншого – сторонній може підглянути код, що набирається. Більш захищеним від несанкціонованого доступу та поширеним є доступ за безконтактними *proximity*-картами. Карта має унікальний номер, за яким СКУД визначає права її власника у системі.

Наступним кроком до абсолютної захищеності стали смарт-картки, для яких існує можливість зберігання ідентифікаційного коду в захищеній області

карти, що перезаписується. Процес обміну картки зі зчитувачем здійснюється за криптозахищеним протоколом, що зводить до нуля ризик підроблення такої картки.

Ще один напрямок, що розвивається – ідентифікація за біологічними ознаками. Найпростіший і найдешевший спосіб – ідентифікація по відбитку пальця. До його недоліків можна віднести високий рівень помилок, коли зчитувач не впізнає користувача, який має право доступу, або сприймає навпаки як правильний чужий відбиток. Крім того, підробляти навчилися і відбитки пальців. Стримує поширеність таких точок доступу та їх низька пропускна спроможність.

Існують пристрої ідентифікації, що поєднують декілька описаних технологій, наприклад, *proximity*-зчитувач з клавіатурою, коли доступ здійснюється за картою та ПІН-кодом. Або біометричну технологію розпізнавань по відбитку пальця і зчитувач смарт-карт (при цьому відбиток зберігається в захищеній області карти, що перезаписується). Користувач підносить картку та прикладає палець до сенсора пристрою, де отриманий відбиток порівнюється з тим, що зберігається у картці.

Контролери мережевих СКУД об'єднані лініями зв'язку та підключені до комп'ютера, що забезпечує централізований збір інформації та управління системою. Це дозволяє забезпечити ряд корисних функцій щодо організації алгоритмів доступу. Одна з них – заборона «подвійного проходу». Усі точки доступу, що обмежують вхід на територію об'єкта, об'єднуються в одну область. При проході людини через одну з точок області система фіксує, що людина на території. Доки ця карта не буде пред'явлена на виході на одній із точок доступу, що входять в область, повторне її пред'явлення на вхід до будь-якої з точок призведе до відмови в доступі. Цей алгоритм дозволяє виключити можливість проходу на територію об'єкта по одній карті кількох людей.

Ще один приклад – тимчасові або гостьові карти, що мають особливий статус у системі, що обмежує їхні права за терміном дії та доступними областями. Карти можуть видаватися на певний термін чи кількість проходів.

Менш поширений спосіб, що застосовується для особливо захищених об'єктів – доступ до приміщення за двома картами.

З розвитком технологій СКУД та вимог до безпеки об'єктів алгоритмів доступу стає дедалі більше.

Поточний стан зон контролюється провідними і бездротовими датчиками (наприклад, датчики вікон, дверей, руху, задимленості). Залежно від типу сигналу вони викликають відповідну реакцію системи керування. У разі несанкціонованого вторгнення система передає тривожний сигнал на пульт охорони, включає звукову та світлову сигналізацію, інформує господаря за допомогою телефонного дзвінка.

1.3 Вимоги до системи контролю управління доступом

СКУД має забезпечувати санкціонований доступ людей, транспорту та інших об'єктів до (з) приміщення, будівлі, зони та території, шляхом ідентифікації особи за комбінацією різних ознак: речовий код (ключі, карти, брелоки); код, що запам'ятовується (клавіатури, кодонабірні панелі та інші аналогічні пристрої); біометричні (відбитки пальців, сітківка очей та інші).

До систем контролю управління доступом пред’являється досить великий список вимог: вимоги до технічного та програмного забезпечення, взаємозв’язок з пов’язаними системами, перспективи розвитку та модернізації, надійність, безпечність та збереження інформації. Розглянемо ці чинники більш детально.

Вимоги до технічного та програмного забезпечення

У склад СКУД повинні входити: пристрої введення ідентифікаційних ознак у складі зчитувачів та ідентифікаторів, пристрої управління (контролери)

у складі апаратних та програмних засобів, пристрої перегороджувальні керовані у складі перегороджувальних конструкцій та виконавчих пристроїв. Контролери СКУД мають бути універсальними та підтримувати різні типи точок доступу. Вони повинні мати додаткові входи для підключення охоронних датчиків, а також додаткові виходи для керування зовнішніми ланцюгами. Контролери повинні підтримувати роботу з біометричними зчитувачами карт доступу.

Програмне забезпечення (ПЗ) СКУД повинне функціонувати під керуванням різних ОС – операційних систем. ПЗ СКУД повинно мати клієнт-серверну архітектуру. Сервер та віддалені робочі місця повинні працювати у розподілених мережах з організацією доменів. ПЗ СКУД має підтримувати інтеграцію з *IP* камерами. Має бути реалізований функціонал запису відео за подіями з можливістю подальшого перегляду відповідних відео фрагментів за логами подій у системі.

Вимоги до характеристик взаємозв'язків СКУД із суміжними системами

ПЗ СКУД повинно мати можливість перспективної інтеграції з можливими новими програмними продуктами. ПЗ СКУД має передбачати можливість повної інтеграції з іншими зовнішніми системами в частині передачі інформації про стан пристроїв, звітів, статистик та ін.; має забезпечувати завантаження/розвантаження структури підрозділів розгалуженої системи.

Перспективи розвитку, модернізації системи

ПЗ СКУД має забезпечувати можливість подальшого розширення системи (кількості контролерів, користувачів у системі, кількості віддалених робочих місць) без необхідності придбання додаткових ліцензій на технічні засоби (контролери), програмні (віддалені робочі місця) та ін. Система повинна мати можливість підключення додаткових засобів ідентифікації та аутентифікації контролю доступу.

Вимоги до надійності

Система повинна зберігати працездатність та забезпечувати відновлення своїх функцій у разі виникнення наступних позаштатних ситуацій:

− при збоях у роботі апаратної частини, що призводять до перезавантаження ОС сервера СКУД. Відновлення повної працездатності серверної частини ПЗ СКУД має відбуватися автоматично після успішного перезапуску ОС;

− при помилках у роботі ПЗ СКУД. При встановленні факту некоректної роботи окремих модулів або всього програмного забезпечення в цілому повинна бути передбачена можливість автоматичного перезапуску окремих процесів або всього програмного забезпечення в цілому;

− при помилках, пов'язаних із програмним забезпеченням сторонніх виробників (ОС, драйвери пристроїв та ін.), відновлення працездатності покладається на ОС.

Контролери СКУД встановлюються всередині об'єкта, що охороняється (захищається) і повинні забезпечувати цілодобовий режим роботи. Гарантійний термін експлуатації програмно-апаратної частини СКУД має бути не менше 12 місяців з дня встановлення обладнання.

Вимоги до безпеки

Система електроживлення контролерів СКУД повинна забезпечувати захисне відключення при перевантаженнях та коротких замиканнях у ланцюгах навантаження, а також аварійне ручне відключення та автоматичне відновлення електроживлення після усунення причини несправності.

Фактори, що надають шкідливі впливи на здоров'я, пов'язані з роботою контролерів СКУД та виконання ними своїх функцій, у тому числі інфрачервоне, ультрафіолетове, рентгенівське та електромагнітне випромінювання, вібрація, шум, електростатичні поля тощо, не повинні перевищувати чинних норм.

Вимоги щодо збереження інформації при аваріях

Програмне забезпечення СКУД має відновлювати своє функціонування під час коректного перезапуску апаратних засобів. Повинна бути передбачена можливість організації автоматичного та (або) ручного резервного копіювання даних системи засобами системного та базового програмного забезпечення (ОС, СУБД), що входить до складу програмно-технічного комплексу.

Висновок до першого розділу

У розділі наведена актуальність систем контролю управління доступом та їх перспективи розвитку, потенціал їх використання у багатьох сферах технічного, економічного та соціального характеру. Здійснено аналіз систем контролю управління доступом та наведені особливості використання автономних, мережевих та універсальних СКУД. Наведені алгоритм роботи системи в залежності від самої точки доступу (двері, турнікети, шлагбауми, шлюзи). Наведено аналіз пристроїв ідентифікації санкціонованого доступу (парольні, біометричні, майнові). Також у розділі наведено обґрунтований список вимог до систем контролю управління доступом: вимоги до технічного та програмного забезпечення, взаємозв’язок з пов’язаними системами, перспективи розвитку та модернізації, надійність, безпечність та гарантоване збереження інформації.

РОЗДІЛ 2
АНАЛІЗ АПАРАТНИХ ПЛАТФОРМ ТА ТЕХНОЛОГІЙ СКУД

2.1Аналіз апаратних платформ управління

Система контролю доступу перетворилася на невід'ємну частину засобів безпеки багатьох підприємств та офісів. Але зараз все більшої популярності набувають системи контролю доступу для дому. Це і прості домофони, і складніші пристрої, інтегровані в систему «Розумний будинок».

З СКУД можна легко контролюватимете вхід до будинку. Якщо у вас є домашній персонал, ви зможете забороняти доступ до певних приміщень. Ви зможете контролювати безпеку своєї дитини. Як тільки дитина скористається системою, ви отримаєте *SMS* про її прихід, а СКУД «Розумний будинок» виконає заплановані дії: відключення сигналізації, включення опалення або вентиляції, блокування телевізорів та комп'ютерів. Тобто найбільш поширеним проектуванням СКУД є реалізація за допомогою системи «Розумний будинок».

Багатофункціональні системи «Розумний будинок», які забезпечують комфорт та безпеку житла, з кожним роком набирають все більшої популярності. По-перше, це пов'язано з підвищенням технологічної грамотності простих людей на тлі розвитку цифрової промисловості. По-друге, таке обладнання поступово дешевшає, що робить його доступнішим для широких мас населення. В даний час системи «Розумний будинок» встановлюються як на житлові, так і на комерційні об'єкти нерухомості: квартири, котеджі, офіси, готелі, *SPA*-центри.

З кожним роком ця сфера дедалі більше розширюється і дедалі більше компаній представляє свої розробки у цій тематиці. На даний момент йде своєрідне змагання між апаратними платформами тематики інтернету речей, розроблених різними виробниками. Кожен із цих виробників розуміє що чим успішніша і ефективніша буде його платформа, тим більший прибуток він

зможе отримати. Сучасний ринок пропонує величезний вибір технічних пристроїв для автоматизації житла, тому порівняєм системи «Розумний будинок» різних виробників.

Розглянемо найбільш популярніші апаратні платформи для реалізації системи контролю доступом на базі «Розумного будинку».

Система *Ajax.* Виробник – Україна, відповідно за замовчуванням підтримується український та російський інтерфейси. Дана система автоматизації будинку повністю справляється відразу з двома важливими завданнями:

− забезпечує комфорт та зручність в управлінні життєзабезпеченням приміщення;

− гарантує безпеку житла повною мірою, контролюючи межі об'єкта на предмет злому, а також електричну, пожежну, газову та інші загрози для будинку.

Устаткування «Розумний будинок» *Ajax* працює на надійно зашифрованому та захищеному двосторонньому радіозв'язку *Jeweller* власної розробки, має повну автономність від електромережі завдяки резервному джерелу живлення – хабу, характеризується стильним дизайном усіх своїх пристроїв.

Переваги: простий монтаж; бездротовий канал зв'язку між системними елементами; широка зона дії сигналу (до 2000 м); наявність захисту від зняття будь-якого датчика (бампера); можливий доступ інших користувачів (повний чи частковий); автономна робота хаба від акумулятора (до 16 години); *Wi-Fi* та *GSM*-зв'язок; різноманітність способів інформування користувача (дзвінок, *SMS, Push*-повідомлення); розумна розетка показує витрату електроенергії (з урахуванням підключених приладів), що автоматично відключається при перепадах напруги; встановлення за QR-кодом та управління за допомогою смартфона (*iOS, Android*); підключення до 100 пристроїв; наявність тривожної кнопки на пульті (брелоку); невисока вартість комплекту (від 200 $).

Недоліки: функціонування лише з роботою центрального контролера (*Hub*), тобто відсутність автономності датчиків; немає власної камери відеоспостереження (але є можливість підключення стороннього обладнання); керування лише через телефон, хоча це знімає необхідність встановлювати будь-які додаткові програми на ПК.

На сьогодні обладнання *Ajax* – одна з найкращих систем «Розумний будинок». Вона багатофункціональна, надійна, зручна, компактна. Має якісний захист від зламів, чудовий дизайн та зрозумілий інтерфейс. Встановлення та налаштування такого комплексу спрощено до мінімуму та цілком доступне навіть для технічно непідготовлених користувачів. Важливою перевагою є і досить демократична ціна на девайс, враховуючи його широкий функціонал.

Система *BroadLink.* Виробник – Китай. За замовчуванням немає українського інтерфейсу, за потреби його можна знайти. Устаткування «Розумний дім» *BroadLink* є комплектом сучасних цифрових пристроїв, створених для раціонального управління побутовою технікою, а також освітлювальною, енергетичною, охоронною та іншими системами в будинку. Кожен елемент такого комплексу може працювати як самостійно, і взаємодіяти один з одним.

Переваги: швидко встановлюється, підключається та налаштовується; має широкий асортимент датчиків (вологості, температури, висвітлення, шуму, забруднення повітря); можна легко додавати та прибирати різні пристрої; функціонує без центрального хаба (автономна робота датчиків); бездротова взаємодія пристроїв між собою; є своя камера відеоспостереження; контролюється через *Wi-Fi* через Інтернет з будь-якої точки планети; демократична вартість обладнання (від 200 $).

Недоліки: невелика дальність дії сигналу (до 50 м); відсутність резервного живлення хаба; пульт працює лише на прийом сигналів.

Система *BroadLink* займає високі позиції завдяки широкому функціоналу, якісному програмному забезпеченню, простоті в установці та користуванні, а

також доступній вартості. Такий комплекс не потребує центрального контролера, адже всі його пристрої хоч і взаємопов'язані, але можуть працювати повністю автономно. Робота побутової техніки в будинку налаштовується згідно зі сценаріями у додатку на смартфоні.

Система *Fibaro.* Виробник – Польща (розробка та реєстрація бренду – США). Важко знайти русифікований інтерфейс. Розумний будинок *Fibaro* відноситься до професійного обладнання для забезпечення автоматизації та безпеки будинку з найширшим функціоналом. Однак, на відміну від багатьох подібних систем, потребує встановлення та налаштування своєї апаратури досвідченими фахівцями.

Переваги: чудове наповнення системи всілякими датчиками та пристроями; наявність камери відеоспостереження; величезний вибір сценаріїв користувача; розсилання повідомлень відразу на кілька телефонів; робота на базі протоколу *Z-Wave*, що дає змогу успішно взаємодіяти з іншим подібним обладнанням; датчик протікання оснащений сиреною; розумна розетка відображає рівень енергоспоживання підключених пристроїв, а також вимикається при стрибках напруги; невелика дальність сигналу системи збільшується за рахунок можливості кожного елемента бути ретранслятором сигналу; голосове керування через сервіс *Google*, але лише англійською мовою.

Недоліки: висока вартість обладнання (від 600 $); тільки професійний монтаж та налаштування; обов'язкове підключення центрального контролера *Fibaro Home Center* до Інтернету через *LAN*-кабель; неможливість функціонування без центрального хаба; відсутність резервного живлення хаба; обмежена дальність сигналу (до 50 м без перешкод, хоча ця проблема розв'язується); затримка *Push*-повідомлень; необхідність обов'язкової установки програмного забезпечення на ПК, а також урізаний мобільний додаток.

У порівнянні з системами «Розумний будинок» інших виробників, обладнання *Fibaro* має найкращу наповненість всілякими датчиками для контролю стану приміщень та забезпечення автоматизації в керуванні

домашньою технікою. Проте встановити та розібратися з таким комплексом допоможе лише професіонал.

Система *Orvibo*. Виробник – Китай. Відсутність українського та російського інтерфейсу за умовчанням (але є англійська), що дещо ускладнює встановлення та налаштування. *Orvibo* – це недорогий комплект простого в експлуатації обладнання, головне завдання якого полягає у забезпеченні безпеки будинку. І тільки в другу чергу така установка може бути базою для організації повноцінної системи «Розумний будинок».

Переваги: простота в установці та підключенні, віддалений контроль через програму на смартфоні; автоматичне знаходження та підключення сенсорів до центрального хабу; широкий вибір пристроїв та можливість масштабування системи (близько 100 датчиків), причому інших виробників; наявність власної відеокамери; бездротовий протокол взаємодії між контролером та датчиками *ZigBee*; автономність деяких пристроїв від центрального хаба; вибір сценаріїв роботи з технікою будинку; *Wi-Fi* зв'язок із телефоном, до 10 номерів; цілком доступна вартість (від 150 $).

Недоліки: невелика зона дії сигналу (до 30 м); досить скромний набір пристроїв у базовій комплектації (тільки часткове охоплення багатокімнатної квартири чи офісу); відсутність резервного живлення хаба у разі відключення електроенергії; дротове підключення до Інтернету (для надійності роботи системи).

Можна сказати, що *Orvibo Security Kit* – це проміжне обладнання між класичною системою охорони приміщення та «Розумним будинком». Воно має просте та зрозуміле живлення, чудові можливості для масштабування пристроями сторонніх виробників за рахунок універсального протоколу *ZigBee*. Однак з метою зробити цю систему доступнішою в плані покупки, тут використовуються досить примітивні датчики без захисту від злому та відключення, а камера розрахована тільки на роботу всередині приміщення.

Система *Xiaomi*. Виробник – Китай. Відсутність українського та російського інтерфейсу за умовчанням, лише англійська та китайська, що накладає свої складнощі в процесі встановлення та налаштування.

Розумний будинок від *Xiaomi* відноситься до бюджетного класу обладнання, яке дозволяє зробити керування різними пристроями та побутовою технікою в будинку максимально простим та зручним.

Переваги: повна автономність пристроїв; можливість масштабування; наявність власної камери відеоспостереження; бездротовий протокол *ZigBee*; зручне керування за допомогою смартфона через *Wi-Fi*; наявність сценаріїв, що настроюються; компактність та стильний дизайн; низька вартість базового комплекту (всього 90 $).

Недоліки: дуже невелика зона впливу сигналу (до 10 м); скромний набір сенсорів та виконавчих пристроїв у базовому наборі; на різні датчики потрібне своє становище; відсутність резервного харчування хаба.

Таким чином, комплект *Xiaomi* є чудовою стартовою платформою для підключення інших сенсорів та пристроїв, у тому числі сторонніх виробників. Її елементи працюють як самостійно, так і як єдине ціле. З їхньою допомогою можна створити досить функціональну систему контролю житлового простору, включаючи забезпечення безпеки. Ця система, враховуючи її вартість, підійде для ознайомлення із системою розумного будинку.

Система *Arduino* – це платформа для додавання та програмування електронних пристроїв з типами управління: ручний, напівавтоматичний та автоматичний. Платформа є конструктором, з прописаними правилами взаємодії елементів між собою. Система відкрита, тому кожен зацікавлений виробник робить внесок у розвиток *Arduino*. Цей продукт підходить для розвинутих користувачів, які мають знання у проектуванні електронних пристроїв. Конструктор *Arduino* добрий тим, що в його системі можна використовувати будь-які елементи розумного будинку від різних виробників. Ця можливість дозволяє платформі не бути обмеженою лише однією

екосистемою розумного будинку, а підбирати будь-які компоненти електроніки для реалізації вирішення власних завдань. Основним елементом розумного будинку є центральна плата мікроконтролера. Для підключення плати до інтернету знадобиться: *Wi-Fi*-адаптер, налаштований на прийом та передачу сигналу через маршрутизатор; або підключений через *Ethernet* кабель, *Wi-Fi* роутер. Також є варіант дистанційного управління з *Bluetooth*. Відповідно, до плати має бути підключений *Bluetooth* модуль. Є кілька варіантів управління розумним будинком *Arduino*: за допомогою програми для смартфона або через веб. Для програмування використовується інтегроване середовище розробки *Arduino – Arduino IDE*.

2.2 Аналіз безпровідних протоколів управління

У наш час рідко хто може довго обходитися без цифрових пристроїв. Сьогодні навіть наші будинки стають цифровими, дозволяючи нам контролювати житло, де б ми не знаходилися: в автомобілі, офісі чи іншій країні. Оскільки будинки стають розумнішими, нам потрібен універсальний спосіб, за допомогою якого всі домашні пристрої будуть спілкуватися між собою і з нами. Нині такої «універсальної мови», на жаль, немає. Натомість ми бачимо кілька конкуруючих і практично несумісних між собою бездротових стандартів «розумного будинку». Кожен із них бореться за звання головної технології управління житлом. До таких стандартів належать не тільки добре знайомі всім *Wi-Fi* та *Bluetooth*, а й спеціалізовані протоколи – *Z-Wave, ZigBee* та *Thread*. Усі вони мають переваги та недоліки, не очевидні з першого погляду. Розглянемо більш детально ці технології.

Протокол *Wi-Fi*. Це найочевидніше рішення для домашньої автоматизації. Це найпоширеніша бездротова мережна технологія з мільярдами користувачів по всій земній кулі. За даними галузевого консорціуму *Wi-Fi Alliance,* за допомогою цього стандарту відбувається передача близько

половини всього світового Інтернет-трафіку. *Wi-Fi* широко використовується у приватних будинках, офісах та громадських місцях. Ця технологія є найбільш популярною для підключення комп'ютерів, смартфонів та планшетів до Світової мережі. Технічно, за допомогою *Wi-Fi* можна з'єднати два пристрої «точка-точка», щоб вони обмінювалися інформацією між собою.

Технологія *Wi-Fi* заснована на сімействі стандартів бездротової мережі *IEEE 802.11x*. Вони визначають лише перші два рівні моделі *OSI* – фізичний та канальний. Мережа *Wi-Fi* має топологію «зірка», а це означає, що всі її вузли з'єднуються безпосередньо з центральним елементом – бездротовим маршрутизатором. У такій топології кінцеві пристрої можна додавати та видаляти з мережі, не впливаючи на цілісність її структури та передачу даних у ній. Але цей підхід створює єдину точку відмови.

Wi-Fi – це потужне та надійне бездротове рішення, яке успішно використовується для побудови локальних мереж уже багато років. 802.11 де-факто став глобальним стандартом зв'язку, оскільки пропонує безліч гнучких функцій та постійно вдосконалюється Інститутом інженерів електротехніки та електроніки (*IEEE*).

Wi-Fi може легко передавати відеопотоки високої чіткості, а теоретична межа його пропускної спроможності набагато вища, ніж потреби середнього користувача. Деякі старіші версії стандарту 802.11 мають обмеження 11 Мбіт/с або 54 Мбіт/с, але 802.11n, що широко використовується зараз, здатний передавати вже десятки і сотні мегабіт в секунду, а більш новий 802.11ac – ще більше. Ці цифри, безумовно, чудово виглядають на тлі інших популярних рішень для домашньої автоматизації. Значення їх пропускної спроможності виражаються у Кбіт/с, а чи не в Мбіт/с. Крім того, одна з головних переваг *Wi-Fi* – повсюдна доступність інфраструктури 802.11. Той факт, що цей стандарт інтегрується в нові ноутбуки, смартфони та планшети, має велике значення з точки зору реалізації керуючих додатків розумного будинку та Інтернету речей.

Протокол *Z-Wave.* Вже понад десять років *Z-Wave* – безперечний лідер серед технологій професіональної автоматизації за кількістю інстальованих пристроїв (понад 100 млн. по всьому світу). Цей протокол бездротового зв'язку з ультранизьким енергоспоживанням спеціально розроблений, щоб дати звичайним користувачам можливість ефективного та надійного віддаленого керування широким спектром датчиків та виконавчих пристроїв розумного будинку.

Z-Wave представлений 2003 року фірмою *Zensys*, придбаною через п'ять років компанією *Sigma Designs*. Наприкінці 2017 року технологія *Z-Wave* стала власністю великої напівпровідникової компанії *Silicon Labs*. Вона ліцензує на взаємну сумісність кожен продукт, який використовує *Z-Wave*, і є основним постачальником модулів та напівпровідникових компонентів *Z-Wave*. Ця технологія перетворилася на загальновизнаний міжнародний стандарт бездротового зв'язку для управління та автоматизації житлових приміщень, але вартість її розробок ще досить достатньо дорога.

Z-Wave охоплює всі рівні мережі *OSI*, від фізичного до прикладного. Це гарантує високий рівень сумісності обладнання домашньої автоматизації від різних постачальників. *Z-Wave* – добре налагоджений протокол, орієнтований обмін короткими командами і повідомленнями між пристроями, що зводить до мінімуму завантаженість радіоканалу і знижує ймовірність втрати даних. *Z-Wave* використовує концепцію пористої топології мережі (*mesh*-мережа). Протокол розроблений таким чином, що вузли мережі, що виконують роль ретрансляторів, мають можливість перенаправляти через себе повідомлення, доки воно не досягне адресата. Такий підхід дозволяє значно розширити радіус дії бездротової мережі, а й підвищує її надійність. У разі переміщення/деактивації/виходу з ладу будь-якого вузла мережа не буде паралізована, а продовжить роботу в штатному режимі: повідомлення почнуть автоматично прямувати через вузли мережі, що ретранслюють, в обхід вузлу, що вийшов з ладу.

Тривалий час *Z-Wave* розвивався як закрита технологія. Це дозволило розробникам гарантувати відмінну сумісність, безпеку, стійкість до відмови і т. д. Але така «закритість» обходиться дорожче в розробці пристроїв. Тому рішення *Z-Wave* не можна назвати бюджетним варіантом для розумного будинку. Інша річ, що ставлення ціна/якість, де технологія *Z-Wave* не залишила конкурентам жодних шансів.

Протокол *ZigBee.* Вже понад десять років *ZigBee* є основним конкурентом *Z-Wave*, ведучи запеклу боротьбу за лідерство на ринку домашньої автоматизації. За цей час *ZigBee*, поряд з *Z-Wave*, став одним з бездротових комунікаційних технологій, що найбільш широко використовуються, в сучасних розумних будинках.

Розвиток *ZigBee* розпочався наприкінці 90-х років минулого століття, але лише у 2004 році його перша специфікація була опублікована галузевим консорціумом *ZigBee Alliance*. Як і *Z-Wave*, це стандарт із низькими показниками швидкості та малим енергоспоживанням, оптимізований для віддаленого моніторингу та управління розумним будинком. Обидва ці стандарти використовують *mesh*-мережі та мають схожі функції. На погляд ці стандарти здаються ідентичними, але за більш детальному розгляді між *ZigBee* і *Z-Wave* виявляються кардинальні відмінності.

Набір протоколів *ZigBee* визначає лише верхні рівні моделі *OSI* – мережевий, транспортний та прикладний. Він побудований поверх стандарту *IEEE 802.15.4*, який визначає нижні рівні бездротової мережі, орієнтованої на кінцеві пристрої (а не користувачів, як, наприклад, *Wi-Fi*), і характеризується низьким енергоспоживанням і низькою швидкістю передачі даних. Стандарт *IEEE 802.15.4* підтримується кількома постачальниками чіпів та використовується не тільки для *ZigBee*, але й кількома десятками інших протоколів. На відміну від *Z-Wave*, яка для доставки пакетів до окремих вузлів мережі використовує схему маршрутизації джерела повідомлення, *ZigBee* використовує маршрутизацію від адресата. Таким чином, у реалізації

mesh-мережі *ZigBee* бере участь три класи пристроїв: координатор («мозок» мережі), маршрутизатор (постійно активний) і кінцеві пристрої (велику частину часу знаходяться в режимі сну). Таким чином, *ZigBee* пропонує дещо відмінний з технічного погляду підхід до організації *mesh*-мережі, але він, як і у випадку з *Z-Wave*, здатний забезпечити самовідновлення мережі та може швидко перенаправити пакети даних, щоб забезпечити їх доставку, якщо будь-який вузол не працює чи не відповідає.

ZigBee – відкритий стандарт бездротового зв'язку, що насамперед виглядає привабливим з погляду розробників та виробників. Це дозволяє їм бути більш гнучкими у виборі необхідної функціональності, а також з меншими витратами виводити на ринок нові продукти. Це розвинена технологія з низьким енергоспоживанням та високою безпекою, але має і деякі недоліки. *ZigBee* погано справляється із ситуаціями, коли в зоні дії мережі існують сильні перешкоди, що створюються іншими пристроями. Також має погану сумісність між пристроями *ZigBee* різних виробників через занадто м'які умови сертифікації, що висуваються консорціумом *ZigBee Alliance.*

Протокол *Thread*. Об'єднання *Thread Group* з'явилося в липні 2014 року з метою створення простої та безпечної мережі з малим енергоспоживанням для розумного будинку та підключених до бездротової мережі пристроїв. Через рік члени організації представили технічні специфікації та документи, що дозволяють створювати продукти на основі *Thread*. Від початку протокол позиціонувався як рішення виключно для сегменту домашньої автоматизації. На перший погляд такий підхід може здатися менш амбітним, ніж, скажімо, у того ж *ZigBee Alliance*. Але початкове звуження цільового ринку мало сенс, оскільки мало дозволити *Thread Group* надати стандарт, ідеально спроектований задоволення потреб конкретної групи замовників.

Thread працює поверх вже згадуваного раніше стандарту радіозв'язку *IEEE 802.15.4*, який у тому числі є основою кожної мережі *ZigBee*. Сам же протокол *Thread* визначає лише мережний та транспортний рівні моделі *OSI,*

призначені для вирішення таких проблем, як маршрутизація, розгортання та забезпечення безпеки.

На основі фізичної інфраструктури 802.15.4 *Thread* увібрав у себе всі її сильні і слабкі сторони, про які ми згадували при розгляді стандарту *ZigBee*. Це низька вартість зв'язку з найближчими пристроями, низький рівень енергії, що споживається, одноканальність рішення з максимальною швидкістю передачі даних 250 Кбіт/с, а також крайня завантаженість робочого діапазону 2,4 ГГц, особливо в міських умовах. Також до недоліків технології треба віднести вкрай повільні темпи впровадження технології.

Протокол *Bluetooth.* Перший крок у бік Інтернету речей було зроблено в 2010 році, з випуском версії *Bluetooth Core 4.0*, що включає версію з низьким енергоспоживанням (*Bluetooth Low Energy, BLE*), відому також як *Bluetooth Smart*. Ця нова технологія була розроблена з орієнтацією на нове покоління розумних пристроїв, багато з яких живляться від батарей і, отже, потребують ефективнішого управління живленням. Але й тоді *Bluetooth* ніхто всерйоз не сприймав як альтернативну технологію домашньої автоматизації.

Як і Z-Wave, Bluetooth охоплює всі рівні основної моделі *OSI* – від фізичного до прикладного рівня. Таким чином, *Bluetooth Special Interest Group* (*SIG*), орган, який контролює розробку та ліцензування *Bluetooth*, має такий самий рідкісний привілей, як і *Z-Wave Alliance,* – безпосередньо та самостійно вносити будь-які зміни до стандарту.

Bluetooth Low Energy, як і інші стандарти зв'язку з низьким енергоспоживанням та низькою пропускною здатністю, орієнтований на передачу даних невеликими пакетами та короткий час роботи пристрою з батарейним живленням в активному режимі. Саме в цьому криється його основна відмінність від звичного нам класичного *Bluetooth*, оскільки пристрої *Bluetooth Low Energy* з'єднуються один з одним лише за необхідності надсилання або отримання даних. Для технології, орієнтованої на низьке енергоспоживання, *Bluetooth Low Energy* має досить вражаючу швидкість

передачі даних – до 1 Мбіт/с (для нової п'ятої версії *Bluetooth* це значення збільшено до 2 Мбіт/с). До недоліків технології слід віднести, що *Bluetooth* використовує той же діапазон 2,4 ГГц, що і багато інших радіотехнологій, включаючи не тільки вже згадані нами *Wi-Fi, ZigBee* і *Thread*, але і безліч інших пристроїв, таких як мікрохвильові печі, радіоняні або бездротові телефони. також треба відмітити недостатню надійність, так як не використовується топологія комірних мереж.

Висновок до другого розділу

У цьому розділі були наведені бездротові технології, які є основою для таких протоколів як: *Wi-Fi, Z-Wave, ZigBee, Thread, Bluetooth Low Energy.* Проведено аналіз переваг та недоліків безпровідних технологій. Наведено аналіз апаратних платформ (контролерів) для проектування інтернету речей, серед яких особлива увага надана платформі *Arduino*, яка дозволяє робити проекти з великою ступеню інтеграції та великою лінійкою компонентів за власними вимогами до проекту. Виходячи із переваг і недоліків було прийняте рішення розробляти систему контролю доступу на платформі *Arduino* з підтримкою бездротового зв’язку *Wi-Fi.*

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

3.1 Обґрунтування вимог до проектування

Практично всі стратегічні об'єкти оснащені системами контролю доступу, найбільш надійними є біометричні СКУД, які забезпечують високу якість аутентифікації. Може використовуватись основний та резервний метод аутентифікації.

Основний метод аутентифікації використовується для штатного входу в систему. Найпоширеніший з них – вхід паролем, що використовується в переважній більшості комп'ютерних систем. Менш поширеним способом є використання апаратних ідентифікаторів, на які записуються ключі доступу або паролі користувача.

Також у корпоративному секторі популярна двофакторна автентифікація. Як правило, під цим розуміється зв'язка з е-токена і пін-коду введеного користувачем, але зустрічаються і більш екзотичні поєднання, що складаються з біометричного сканера та апаратного ідентифікатора або пароля користувача.

Резервний метод аутентифікації використовується у разі втрати пароля або е-токена, або злому облікового запису. У цьому разі набувають чинності резервні методи аутентифікації. Втім, це не так методи аутентифікації, як механізми скидання пароля.

Найбільш поширені два методи: відповідь на «секретне питання» та відправлення пароля на довірену поштову скриньку, вказану при реєстрації. Ці методи входять в стандартний набір будь-якого інформаційного сервісу, що поважає себе.

Використовуваний фактор аутентифікації – аутентифікація є процес порівняння інформації, що надається користувачем, з еталонною. Залежно від

типу інформації її можна віднести до одного з трьох основних факторів, або їх комбінації.

Таким чином усі системи захисту та контролю доступу поділяють на три групи:

1. Парольна аутентифікація (фактор знання).
2. Апаратна аутентифікація (речовий фактор).
3. Біометрична аутентифікація (біофактор).

Парольна аутентифікація – перший і найпоширеніший на даний момент механізм автентифікації. Це введення чогось, що відомо тільки користувачеві, наприклад, пароля або відповіді на секретне запитання. Теоретично, це найпростіший і безпечніший метод автентифікації, так як він має достатню криптостійкість, його просто і дешево реалізувати, а все що потрібно від користувача, так це запам'ятати 8-12-ти символьну комбінацію з літер, цифр і різних знаків. Проте, практично все зовсім інакше.

Користувачі, як правило, задають слабкі паролі, що пов'язано з самою фізіологією людини, точніше її мозку. Наше мислення асоціативно і безпосередньо пов'язане з промовою, ми мислимо образами, кожен з яких має назву, тому як пароль ми вибираємо назву одного з них. Таким чином більшість паролів, що задаються користувачами, ми можемо знайти у звичайному словнику, а тому вони легко підбираються методом перебору за словником.

Зі зростанням складності пароля він все важчий для запам'ятовування. А зі зростанням кількості облікових записів від різних комп'ютерних систем, яких з кожним роком стає все більше, ситуація ще більше посилюється. Крім того, зі збільшенням складності паролів збільшується кількість помилок при його введенні.

Апаратна аутентифікація – другий за популярністю фактор аутентифікації. Насамперед під цим розуміються апаратно-програмні системи ідентифікації та аутентифікації (СІА) або пристрої введення ідентифікаційних

ознак. До складу СІА входять апаратні ідентифікатори, пристрої введення-виведення (зчитувачі, контактні пристрої, адаптери, роз'єми системної плати та ін.) та відповідне ПЗ. Ідентифікатори призначені для збереження унікальних ідентифікаційних ознак. Крім цього, вони можуть зберігати та обробляти конфіденційні дані. Пристрої введення-виводу та ПЗ здійснюють обмін даними між ідентифікатором і системою, що захищається.

У електронних СІА ідентифікаційні ознаки подаються у вигляді цифрового коду, що зберігається у пам'яті ідентифікатора. За способом обміну даними між ідентифікатором та пристроєм введення-виведення електронні СІА поділяються на:

1. Контактні:

- *iButton – information button* – інформаційна «таблетка»;
- смарт-картки – інтелектуальні карти;
- *USB*-ключі або *USB*-токени (*token* – розпізнавальна ознака, маркер);

2. Безконтактні:

- *RFID*-ідентифікатори – *radio-frequency identification* – радіочастотні ідентифікатори;
- смарткарти*;*
- мобільний прилад (смартфон, планшет).

Контактне зчитування має на увазі безпосередній дотик ідентифікатора з пристроєм вводу-виводу. Безконтактний (дистанційний) спосіб обміну не вимагає чіткого позиціонування ідентифікатора та пристрою вводу-виводу. Читання або запис даних відбувається при піднесенні ідентифікатора на певну відстань до вводу-виводу. Або відстань може бути необмеженою, якщо мобільний прилад використовується по протоколу безпровідної передачі *Wi-Fi,* а не за технологією *NFC* (*near field communication*, зв'язок близької дії).

СІА на базі смарт-карт та радіочастотних ідентифікаторів можна віднести за часом їх створення до старшого, *iButton* – до середнього, а *USB*-ключів – до молодшого покоління.

При обговоренні надійності СІА зазвичай розглядають найважливішу і водночас найслабшу ланку системи – ідентифікатор. У свою чергу, надійність ідентифікаторів пов'язують зі ступенем їхньої захищеності від механічних впливів, впливу температури, зовнішніх електромагнітних полів, агресивних середовищ, пилу, вологи, а також від атак, спрямованих на розтин чіпів, що зберігають секретні дані.

Розробники ідентифікаторів *iButton* забезпечують збереження характеристик своїх виробів при механічному ударі 500g, падінні з висоти 1,5 м на бетонну підлогу, робочому діапазоні температур від –40 до +70 °С, вплив електромагнітних полів та атмосфери. Цьому сприяє герметичний сталевий корпус ідентифікатора, що зберігає міцність при мільйоні контактів з пристроєм введення-виведення. Термін експлуатації ідентифікатора *iButton* складає 10 років. До недоліків СІА на базі *iButton* слід віднести відсутність інтегрованих в ідентифікатори криптографічних засобів, що реалізують шифрування даних при їх зберіганні та передачі в комп'ютер. Тому *iButton* зазвичай використовується разом з іншими системами, які покладаються функції шифрування.

Звичайно, за ступенем механічної надійності радіочастотні ідентифікатори, смарт-картки та *USB*-ключі поступаються *iButton*. Вихід з ладу карти внаслідок механічних пошкоджень є не такою вже рідкісною подією. Вузьким місцем *USB*-ключів є і ресурс їх *USB*-роз'ємів. Розробники даних ідентифікаторів навіть включають цей показник до технічних специфікацій виробів. Перевага радіочастотних ідентифікаторів, смарт-карт і *USB*-ключів полягає в тому, що до їх складу входять захищена енергонезалежна пам'ять і криптографічний процесор, що дозволяють підвищити рівень захисту пристроїв.

Загалом через вартість апаратних ідентифікаторів вони застосовуються в основному в тих сферах, де потрібні зручність, надійність і висока криптостійкість. Основних мінусів всього два: їх можна відібрати або втратити і вони можуть зламатися.

Біометрична аутентифікація використовує біометричні дані, для зняття яких, як правило, необхідні спеціальні програмно-апаратні засоби – так звані, біометричні сканери, які різняться за характером даних, що зчитуються.

Біометричні сканери, що базуються на статичних методах:

1. Розпізнавання відбитків пальців. Це найпоширеніший статичний метод біометричної ідентифікації, в основі якого лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетворюється на цифровий код (згортку) і порівнюється з введеним шаблоном (еталоном) або набором шаблонів.

2. Розпізнавання за геометрією руки. Даний статичний метод побудований на розпізнаванні геометрії кисті руки, що також є унікальною біометричною характеристикою людини. За допомогою спеціального пристрою, що дозволяє отримувати тривимірний образ кисті руки (деякі виробники сканують форму декількох пальців), виходять вимірювання, необхідні для отримання унікального цифрового згортки, що ідентифікує людину.

3. Розпізнавання райдужної оболонки ока. Цей метод розпізнавання ґрунтується на унікальності малюнка райдужної оболонки ока. Для реалізації методу необхідна камера, що дозволяє отримати зображення ока людини з достатньою роздільною здатністю, та спеціалізоване програмне забезпечення, що дозволяє виділити з отриманого зображення малюнок райдужної оболонки ока, за яким будується цифровий код для ідентифікації людини.

4. Розпізнавання геометрії обличчя. Цей спосіб має широке поширення, проте для точності вимагає можливість шаблоном враховувати багато варіантів зображення при зміні зовнішніх обставин, освітлення, позиції обличчя та настрою людини.

Біометричні сканери, засновані на динамічних методах:

1. Розпізнавання за рукописним почерком. Як правило, для цього динамічного методу ідентифікації людини використовується його підпис (іноді написання кодового слова). Цифровий код ідентифікації формується за

динамічними характеристиками написання, тобто для ідентифікації будується згортка, в яку входить інформація щодо графічних параметрів підпису, тимчасових характеристик нанесення підпису та динаміки натиску на поверхню залежно від можливостей обладнання (графічний планшет, екран кишенькового комп'ютера тощо.

2. Розпізнавання за клавіатурним почерком. Метод загалом аналогічний вищеописаному, проте замість підпису у ньому використовується якесь кодове слово, та якщо з устаткування потрібно лише стандартна клавіатура. Основна характеристика, якою будується згортка для ідентифікації, – динаміка набору кодового слова.

3. Розпізнавання голосу. В даний час розвиток цієї однієї з найстаріших технологій прискорився, оскільки передбачається її широке використання при спорудженні інтелектуальних будівель. Існує досить багато способів побудови коду ідентифікації за голосом: як правило, це різні поєднання частотних та статистичних характеристик останнього.

Загалом багатьом із перерахованих методів необхідно досить дороге устаткування й щонайменше дороге ПЗ. Є досить непогані розробки в цій галузі, але вони ще не скоро стануть таким же стандартом, як і вище перераховані методи. Більше того, з розвитком технологій роль біометрії як засобу аутентифікації буде зменшуватися, оскільки отримати зловмиснику доступ до таких даних стає простіше. Голос можна записати, обличчя та очі сфотографувати, а відбитки пальців відсканувати. Потім створити комп'ютерну модель і роздрукувати маску на 3*D* принтері. У результаті біометрія стане переважно засобом ідентифікації.

Класифікація методів ідентифікації систем контролю управління доступом наведена на рис. 3.1.

Опираючись на обґрунтовану класифікацію та вимоги ринку систем контролю управління доступом можна зробити наступні висновки: парольна ідентифікація найбільш проста, але вона сама незахищена; біометрична ідентифікація найбільш захищена, але потребує дорогих спеціалізованих

програмно-апаратних засобів; найбільш поширена апаратна безконтактна ідентифікація.

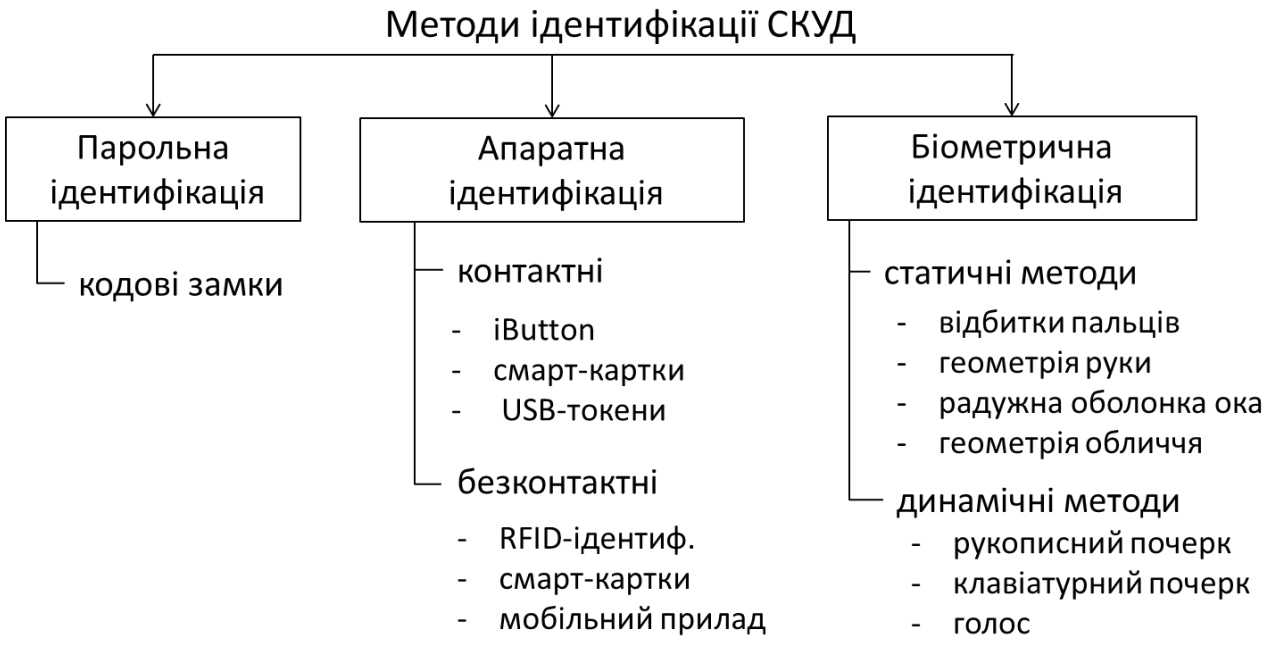

Рисунок 3.1 – Класифікація методів ідентифікації СКУД

При виборі методу ідентифікації у системі контролю доступу виходимо із обміркувань простоти використання, наявності додаткових пристроїв ідентифікації та звісно вартості. Таким чином цим вимогам відповідає апаратний безконтактний метод ідентифікації за допомогою мобільного пристрою (смартфону). Виходячи с того, що цей метод не потребує додаткового апаратного забезпечення, так як кожен сучасний користувач має смартфон. Телефон може мати кілька різних віртуальних карт доступу, що дозволить власнику пристрою отримати доступ до кількох місць. Зв'язок з інтернетом дозволяє реалізовувати оперативну видачу або відкликання карт доступу і перепусток. Це дозволяє позбутися необхідності носити з собою ключі, карти та інші засоби доступу в необхідні місця. Таким чином, телефон стає ефективною та зручною заміною іншим пристроям.

3.2 Розробка технічного завдання та структурної схеми

Сьогодні на ринку є досить великий вибір систем контролю та управління доступом іноземного виробництва. Найбільш доцільним основним параметром для оцінювання оптимальності моделі СКУД є вартість системи конкретного виробника для реалізації типових або однакових функцій. Найбільш доцільним основним параметром для оцінювання оптимальності моделі СКУД є вартість системи конкретного виробника для реалізації типових чи однакових функцій.

Задача роботи – розробити систему, яка дозволить управляти електромагнітним замком для вхідної двері. При проектуванні необхідно вирішити наступні технічні завдання:

- реалізувати апаратну частину управління системою;
- реалізувати програмну частину управління системою;
- забезпечити роботу системи при відключенні живлення;
- забезпечити світове та звукове сповіщення про проходження ідентифікації особи;
- врахувати можливість подальшої модернізації системи (встановлення додаткових пристроїв ідентифікації, підключення систем контролю безпеки і т.д).

Для реалізації технічного завдання треба розробити структурну схему управління замком через *Wi-Fi*, вибрати електронні компоненти та розробити функціональну схему, розробити алгоритм та програму для управляння мікроконтролером.

Живлення системи здійснюється від 10 сонячних модулів, які мають бути встановлені на місці, доступному для сонячного світла. Дані модулі в свою чергу заряджають блок живлення, який складається з 8 літієвих акумуляторів. Для здійснення бездротового зв'язку пристрою введення даних користувача та системи управління та контролю доступом використовуватиметься *Wi-Fi* модуль. Так як *Wi-Fi* модуль працює з напругою 3.3 В, то буде використовуватися перетворювач напруги 12 – 3.3 Вольт, для перетворення 12 В блоку живлення в 3.3 В для живлення модуля. Також, виводи модуля

підключаються до виходів *RX* та T*X* контролера через дільник напруги. Для відтворення звукового та світлового сигналів будуть використовуватися п'єзодинаміки та світлодіоди, підключені безпосередньо до робочих виходів контролера. Об'єктом управління даної системи є електромеханічний замок. Для управління електромеханічним замком потрібно електромагнітне реле, що замикає ланцюг із замку та блоку живлення, т.як. вихідної напруги контролера не вистачить для керування замком.

На рис. 3.2 представлено структурну схему електронного замку з керуванням через *Wi-Fi*.

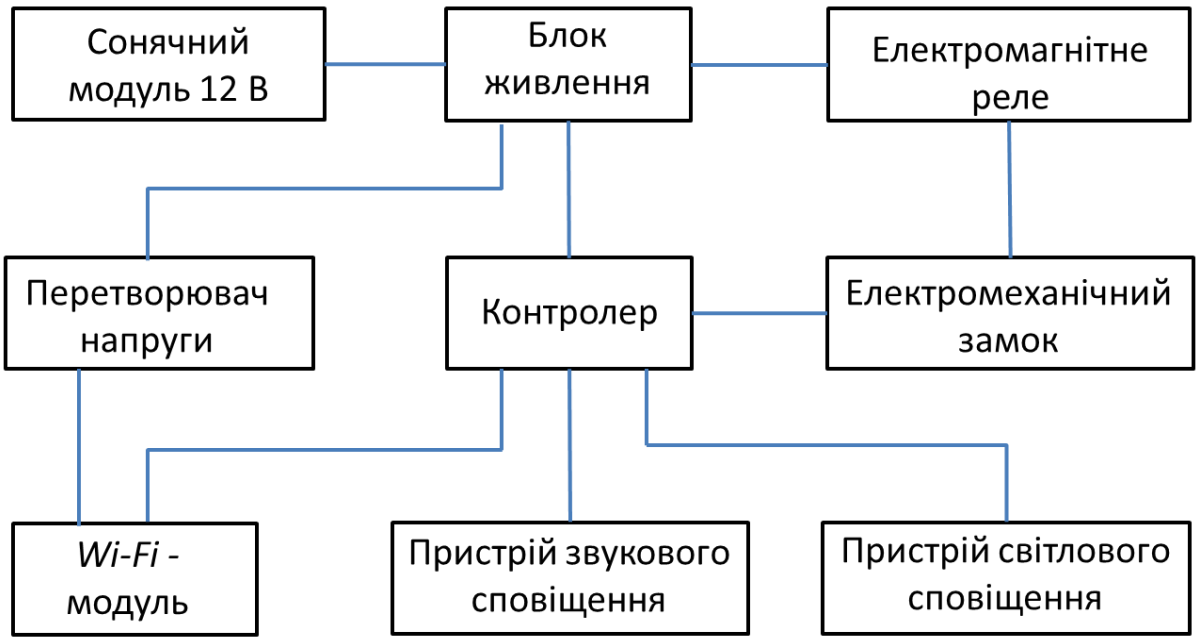

Рисунок 3.2 – Структурна схема управління електромеханічним замком

Робота електромагнітного замку заснована на взаємодії електромагніту та металевої пластини. Використання такого типу замку найбільше виправдане для систем, які відрізняє висока інтенсивність проходів. Відмінною особливістю роботи електромагнітного замку є потреба у постійній подачі електроживлення. У разі вимкнення електроенергії замок відмикається.

Електромеханічні замки мають найрізноманітніші конструкції, у т.ч. для прихованої установки. Такі замки споживають значно менше електроенергії, ніж електромагнітні. Так як для замикання або відкривання потрібно привести в

дію невеликий запірний елемент. Часто електромеханічні замки інтегруються в загальний замок та не вимагають додаткових монтажних робіт. Для його роботи не потрібна постійна подача електроживлення. У конструкції замку є пружина, яка в момент закриття зводиться (звідси назва «замок взводного типу») і залишається в такому положенні до подачі напруги. Електроенергія, таким чином, використовується тільки в момент спрацьовування замку. При відключенні електроенергії замок залишається у закритому положенні, відкрити його можна механічним ключем. Моделей електромеханічних замків багато. Усі вони вигідно відрізняються доступною ціною.

У кожних замків є свої плюси та мінуси, свої особливості та сфери застосування. Але вважається, що електромеханічні замки розвиваються більш стрімко та технологічніше.

3.3 Вибір електронних компонентів та розробка функціональної схеми системи управління

У даній системі контролю та управління доступом у ролі пристрою, що приймає рішення, щодо дозволу або заборони доступу в приміщення, використовується *Arduino UNO* на базі мікроконтролера *ATmega 328* (рис. 3.3). *Arduino UNO* – середніх розмірів плата із власним процесором та пам'яттю. Основа – мікроконтролер *ATmega328*. В наявності 14 цифрових входів/виходів (6 з них можна використовувати як ШІМ виводи), 6 аналогових входів, кварцовий резонатор 16 МГц, *USB*-порт (на деяких платах *USB-B*), роз'єм для внутрішньосхемного програмування, кнопка *RESET*. Флеш-пам'ять – 32 Кб, оперативна пам'ять (*SRAM*) – 2 Кб, енергонезалежна пам'ять (*EEPROM*) – 1 Кб.

Вибір саме мікроконтролера, а не одноплатного комп'ютера обгрунтовується поставленим перед системою завданням, а саме управлінням електромеханічним замком. Так як мікроконтролери можуть виконувати тільки одну задачу, задану програмою користувача, в нашому випадку це управління замком, а одноплатні комп'ютери виконують кілька програм в рамках

операційної системи, то немає необхідності використовувати більш складні, потужні та дорогі платформи. Тому в даному проекті використовуватиметься мікроконтролер *Arduino UNO*. Також платформа *Arduino* має дуже зручне середовище програмування *Arduino IDE*, яке має монітор порту, за допомогою якого можна керувати *Wi-Fi* модулем за допомогою *AT*-команд.

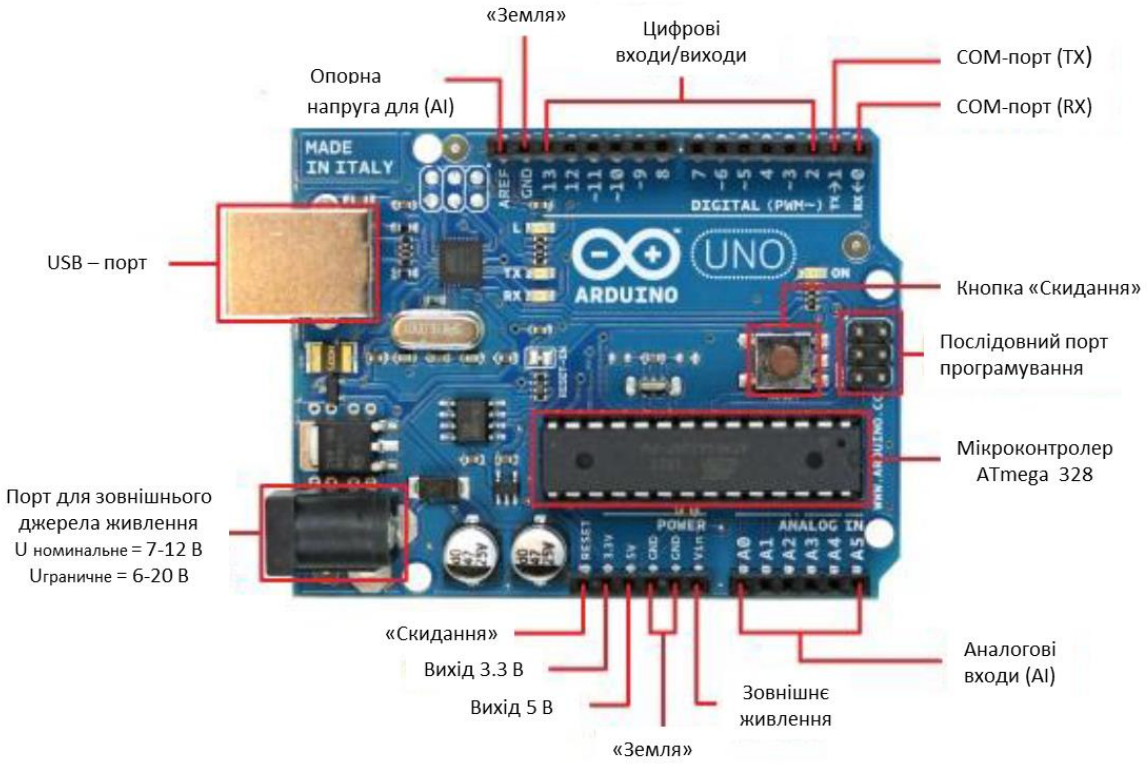

Рисунок 3.3 – Плата *Arduino UNO*

Від контролера нам знадобиться чотири цифрові виходи. Три виходи – для подачі сигналу 5 В на пристрої світлового та звукового оповіщення та один – для подачі сигналу на електромагнітне реле. Для обміну даними з *Wi-Fi* моделлю будуть використовуватися *RX-TX* виходи. Також необхідний вихід *GND*. Сама плата повинна живитися від напруги 12 В. Виходячи з вищенаписаного, найкращим вибором буде плата *Arduino UNO*. Конкурентом їй може стати плата *Arduino DUE*, але ця плата програє *UNO* за ціною, при цьому має додаткові функції, які не потрібні в нашому проекті.

Для реалізації функціональної схеми вибираємо наступні електронні компоненти:

1. *Arduino UNO* на базі процесора *ATmega328*.

2. *Wi-Fi* модуль *ESP8266-01*.

3. Електромагнітне реле *srd-05vdc-sl-c*.

4. Перетворювач напруги *AMS1117*.

5. Електромеханічний замок «*ATIS Lock G*».

6. Сонячний модуль 6В, 1 Вт– 10 шт.

7. Акумулятори літієві 18650 3.7В, 2600 мАч – 8 шт.

8. П'єзовипромінювач звуку *HPA17A* 5В, 25мА.

9. Світлодіод зелений *510PG2C* 3В, 20мА.

10. Світлодіод червоний *510HR3C* 2.6В, 20мА.

11. *C1-4* резистор 0,5 0,25 Вт, 5%, 150 Ом.

12. *C1-4* резистор 0,25 Вт, 5%, 220 Ом.

13. *C1-4* резистор 0,25 Вт, 5%, 100 Ом.

14. Діод *1N4007* 1А, 1000 В.

Максимальний струм на виходах *Arduino UNO* складає 40мА. Це недостатньо для керування *WI-FI* модулем *ESP8266-01*, який може споживати від 62 до 215 мА, залежно від режиму роботи. Отже, його не можна підключити для живлення до виходу 3,3 В контролера. Але, можна підключити цей модуль до блоку живлення системи, попередньо знизивши напругу до 3,3 Вольт, необхідних для живлення модуля. Для вирішення цієї проблеми можна скористатися перетворювачем напруги *AMS1117* він перетворює напругу 12 В на 3.3 В. Даний модуль може видавати при 3,3 В струм до 1 А. При цьому, максимальна вхідна напруга може досягати 18 В.

За допомогою *WI-FI* модуля *ESP8266-01* в нашій системі контролю та управління доступом здійснюється зв'язок між користувальницьким пристроєм введення даних для відкриття замку і контролером *Arduino UNO*. На рис. 3.4 представлений зовнішній вигляд модуля *ESP8266-01*.

ESP8266 підключається до послідовного порту *Arduino UNO*, який представлений виходами *RX TX*. Модуль *ESP8266-01* живиться від напруги 3.3 В, яка подається на вихід модуля *VCC* через перетворювач напруги.

Рисунок 3.4 – *WI-FI* модуль *ESP8266-01*

Вихід *GND* – це земля (мінус живлення). *RST* – вихід для перезавантаження модуля. При подачі напруги на нього модуль перезавантажується. Обмін даними між модулем та контролером здійснюється через виходи *RX* (прийом даних) та *TX* (передача даних). У плати *Arduino UNO* на виході *TX* значення напруги при одиниці дорівнює 5 В. Така напруга, подана на вхід *RX* модуля, може вивести його з ладу. Щоб цього не сталося можна використовувати дільник напруги, що складається з двох резисторів: 110 КОм і 200 КОм, який буде перетворювати 5 В на 3,3 В, які будуть подаватися на вихід *RX* модуля. Максимальна дистанція зв'язку – 100 метрів.

Напруга живлення електромеханічного замку становить 12 В. Так як *Arduino UNO* не може забезпечити таке значення напруги на своїх виходах, замок необхідно підключити до блоку живлення 12 В.

Живлення системи здійснюватиме десять сонячних модулів. Напруга на виході кожного модуля становить 6 В, потужність 1 Вт. Для забезпечення 12 В модулі будуть розділені на п'ять пар, в яких модулі будуть з'єднані послідовно. Потім, п'ять пар модулів будуть з'єднані паралельно. Таким чином, ми отримаємо джерело живлення 12 В потужністю 10 Вт.

Так як вся наша система споживає приблизно 4 Вт (*ESP 8266* – 0,825 Вт, *Arduino UNO* – 0,48 Вт, два світлодіода та резистори – 0,3 Вт, п'єзовипромінювач – 0,02 Вт, реле – 0,96 Вт, електромеханічний замок – 0,96 Вт), то для роботи

системи протягом 12 годин нам необхідний блок живлення ємністю мінімум 4800 мАгод.

Для того, щоб система, що розробляється, не залежала від ступеня освітленості навколишнього середовища, необхідна наявність пристрою, який би приймав заряд від сонячних модулів, накопичував його і віддавав його для живлення системи. Даний пристрій – блок живлення і складається з послідовно і паралельно з'єднаних 8 літієвих акумуляторів 18650 3.7В 2600 мАгод. Таким чином, ми отримаємо блок живлення який забезпечить нашу систему необхідними 7 Вт на 12 годин роботи протягом темного часу доби. Максимальний струм розрядки даних акумуляторів може досягати 4,6 А. Для того, щоб за відсутності освітлення, коли на сонячних модулях напруга може опускатися нижче 12 В, струм не був направлений від блоку живлення до сонячних модулів, буде використаний діод *1N4007*. Його максимальна зворотна напруга = 1000 В. Прямий струм 1А.

Крім подачі напруги на *WI-FI* модуль та контролер, напруга подаватиметься і на електромеханічний замок через реле *srd-05vdc-sl-c.* Цей модуль реле має три виводи: *IN*, *DC+*, *DC–*. На вивід *IN* подається керуючий сигнал з контролера. *DC–* вивід для землі, він підключається до виходу *GND* контролера. До виводу *DC+* підключається вивід 5 V контролера. Також реле має ще три виводи: *NO*, *COM* і *NC*. *COM* вивід – це загальний контакт, до нього буде підключений один з контактів ланцюга "блок-замок". *NO* – це нормально-розімкнутий контакт. *NC* – нормально-закритий. Наш електромеханічний замок є нормально відкритим, тобто, він відкривається при знятті з нього напруги. Отже, другий контакт ланцюга блок-замок необхідно підключити до виводу *NC*. Таким чином, якщо керуючий сигнал на виході *IN* реле відсутній, то ланцюг, що складається з блоку живлення замку, буде замкнутий контактами *COM* і *NC*. Отже, на нього надходитиме необхідна напруга щоб замок був закритий. При подачі керуючого сигналу з контролера на вхід *IN* реле, ланцюг, блок живлення і замок буде розмикатися, і замок буде відкритий.

Для того, щоб користувач дізнався, відкрився замок чи ні будуть використовуватися світлодіоди. Якщо ідентифікатор, введений користувачем правильний, то замок відкриється і загориться зелений світлодіод. У решті випадків горітиме червоний світлодіод. Дані світлодіоди споживають струм, що дорівнює 20 мА. Світлодіоди мають дві ніжки. Одна коротка-катод. Довга – анод. Для обмеження струму, що проходить через них від виходів контролера, кожен буде підключений через резистор. Червоний світлодіод споживає струм 20 мА при напрузі 2–2.6 В. Він буде підключений до виводу контролера через резистор 150 Ом. Розсіювана потужність на резисторі складе 0.06 Вт. Зелений світлодіод підключається до наступного виводу контролера і споживає струм 20 мА при напрузі 3 В. Він підключається через резистор 100 Ом і розсіювана потужність на ньому становитиме 0,04 Вт.

Для звукового сповіщення про відкриття замку використовуватиметься п'єзовипромінювач звуку *HPA17A* 5В, 25мА. Так як струм, який він споживає дорівнює 25 мА, то він буде безпосередньо підключений до виходів контролю. Діаметр корпусу випромінювача складає всього 9,6 мм, що робить його дуже компактним. Рівень звуку складає 78дБ. Був обраний саме п'єзовипромінювач, а не електромагнітний випромінювач, так як він має більшу зносостійкість. Також, не має сторонніх шумів і споживає менший струм, порівняно з електромагнітним випромінювачем.

3.3.1. Підключення *Wi-Fi* модуля

У цьому проекті використовується мікроконтролер *ESP8266* з інтерфейсом *Wi-Fi* та *UART*. Існують різні варіанти виконання плат з цим контролером. Всі вони відрізняються лише розмірами, варіантами антен та виходами. Тому в цій роботі використовується *Wi-Fi* модуль *ESP8266 01*.

Цей модуль підтримує протокол передачі даних *UART*. *UART* – це асинхронний послідовний протокол, який передає та приймає дані у вигляді 0 та 1. Синхронізація здійснюється за часом, що визначається до початку передачі

даних. Тому пристрій, що приймає, і передавальний повинен працювати на одній швидкості передачі даних, інакше дані можуть бути або частково, або повністю втрачені. На початку передачі передавальний пристрій посилає логічний нуль. Це – стартовий біт. Приймаюча сторона, отримавши стартовий біт, вичікує певний час і починає зчитувати 2,3,4 і т.д. біти через однакові інтервали часу. Останній біт є стоп бітом, який сигналізує про кінець передачі даних. Для передачі даних використовуються 8 біт плюс біт старту та біт закінчення передачі.

Працювати з *ESP8266* може двома способами:

1. Для керування модулем використовувати перехідник *USB-UART*. Тоді, модуль можна підключити через перехідник до *USB*-порту комп'ютера і керувати ним за допомогою *AT*-команд.

2. Підключити модуль через *UART* до послідовного інтерфейсу *UART Arduino UNO*. А *Arduino UNO*, у свою чергу, підключити до *UAB*-порту комп'ютера, оскільки сама плата контролера вже має перетворювач *USB-UART TTL CH340G*. Управління модулем здійснюватиметься за допомогою АТ-команд за допомогою середовища програмування *Arduino IDE*.

У цьому проекті використовується другий варіант.

Модуль *ESP8266 01* має 8 виводів, які представлені на рис. 3.5.

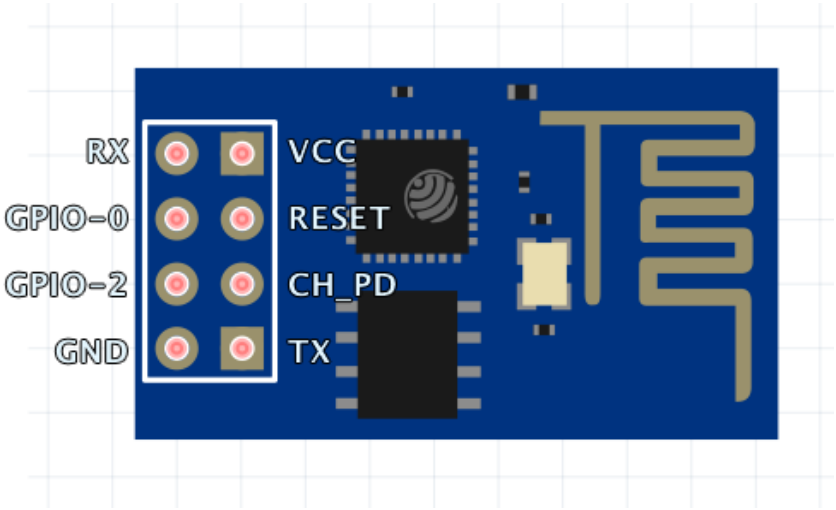

Рисунок 3.5 – Позначення виводів *Wi-Fi* модуля *ESP8266 01*

На вивід *VCC* подається напруга живлення модуля. Для його роботи потрібна напруга 3,3 В. На платі *Arduino UNO* є вивід 3,3 В, але він не підійде для живлення модуля, тому що максимальний струм, який може споживати ESP8266 01, становить 250 мА, в той час, як максимальний струм, який може забезпечити Arduino UNO, становить 40 мА. Тому для живлення модуля використовується блок живлення на 12 В, напруга якого перетворюється за допомогою перетворювача напруги *AMS1117* в 3.3 В, і який може забезпечити максимальний струм 1 А. Вивід *GND* модуля підключається до землі перетворювача *AMS1117*. Вивід *CH_PD* необхідний включення модуля. Для цього на нього необхідно подати напругу, як і на вивід *VCC*. Він також підключається до контакту 3,3 В перетворювача *AMS1117*. Виводи *RX* і *TX* представляють собою передавальну (*TX*) і приймаючу (*RX*) лінії *UART*. Вони використовуються для послідовної передачі даних між модулем і платою *Arduino*. Виввід *TX* модуля необхідно підключити до виводу *RX* контролера. Вивід же *TX* контролера не можна підключати безпосередньо до виводу *RX* модуля. *Arduino UNO* працює на *TTL* логіці (0-5 В), в той час як *ESP8266* працює з 3,3 В. Отже, напруга на виводі *TX* контролера може оказатися занадто великою для модуля і вивести його з ладу. Для вирішення цієї проблеми використовується дільник напруги з резисторів 220 Ом і 430 Ом, зображений на рис. 3.6. Земля дільника – це земля контролера. Виводи *RESET*, *GPIO-0*, *GPIO-2* не використовуються, оскільки потрібні тільки під час перепрошивки модуля.

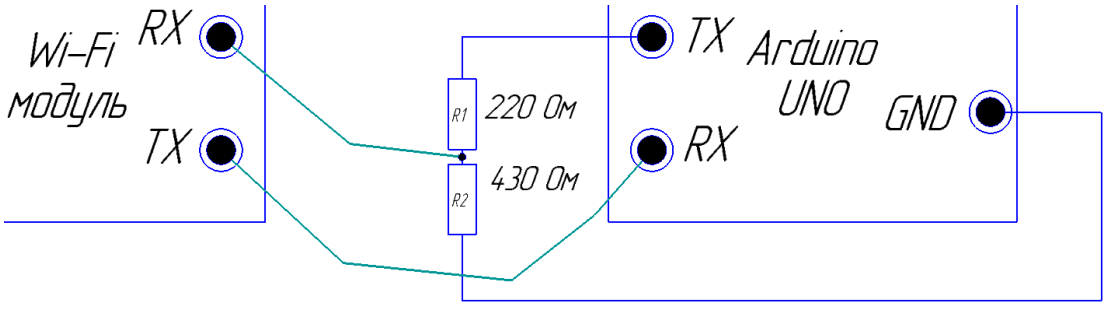

Рисунок 3.6 – Підключення дільника напруги для передачі даних по інтерфейсу *UART*

Напругу дільника розрахуємо по формулі (3.1) і переконаємось, що опіри резисторів вибрані правильно.

$$U_1 = \frac{U_2.R_2}{R_1+R_2} \tag{3.1}$$

$$U_1 = \frac{5\ B * 430\ \text{Ом}}{220\ \text{Ом} + 430\ \text{Ом}} = 3{,}3\ \text{В}.$$

У кінцевому підсумку функціональна схема підключення *Wi-Fi* модуля до *Arduino UNO* буде виглядати так, як показано на рис. 3.7.

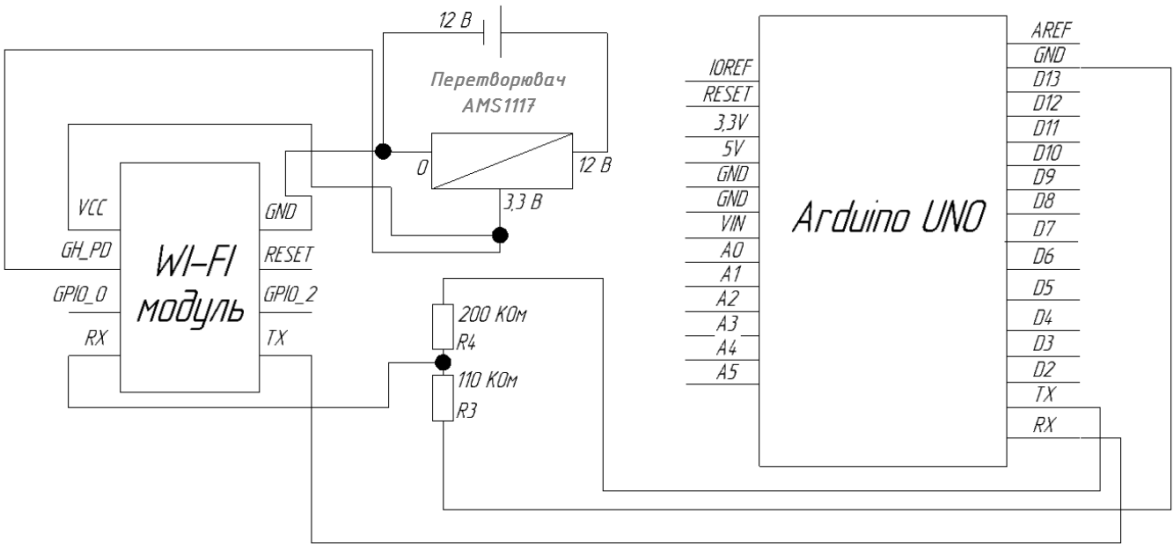

Рисунок 3.7 – Функціональна схема підключення модуля *Wi-Fi*

3.3.2. Підключення електромагнітного реле

Так як максимальний струм і напруга, які може видати *Arduino UNO* недостатні для живлення електромеханічного замку, то в даному проекті використовується електромагнітне реле *srd-05vdc-sl-c*. Даний модуль буде керуватися за допомогою сигналу керування з *Arduino UNO*. Напруга для роботи самого замку надходитиме з блока живлення 12 В, після замикання необхідних контактів реле.

Цей модуль реле має три виводи: *IN*, *DC+*, *DC-*. На вивід *IN* подається керуючий сигнал із контролера. *DC-* вивід для землі, він підключається до виходу *GND* контролера. До виводу *DC+* підключається вивід 5 V контролера.

Також реле має ще три виводи: *NO, COM* і *NC*. *COM* вивід – це спільний контакт, до нього буде підключено один із контактів ланцюга “блок-замок”. *NO* – це нормально-розімкнутий контакт. *NC* – нормально-закритий.

Наш електромеханічний замок є нормально відкритим, тобто він відкривається при знятті з нього напруги. Отже, другий контакт ланцюга блок-замок необхідно підключити до виводу *NC*. Таким чином, якщо керуючий сигнал на виході *IN* реле відсутній, то ланцюг, що складається з блоку живлення замка, буде замкнутий контактами *COM* і *NC*. Отже, на нього надходитиме необхідна напруга, щоб замок був закритий. При подачі керуючого сигналу з контролера на вхід *IN* реле, ланцюг блока живлення і замка буде розмикатися, і замок буде відкритий.

Принципова схема підключення реле показана рис. 3.8.

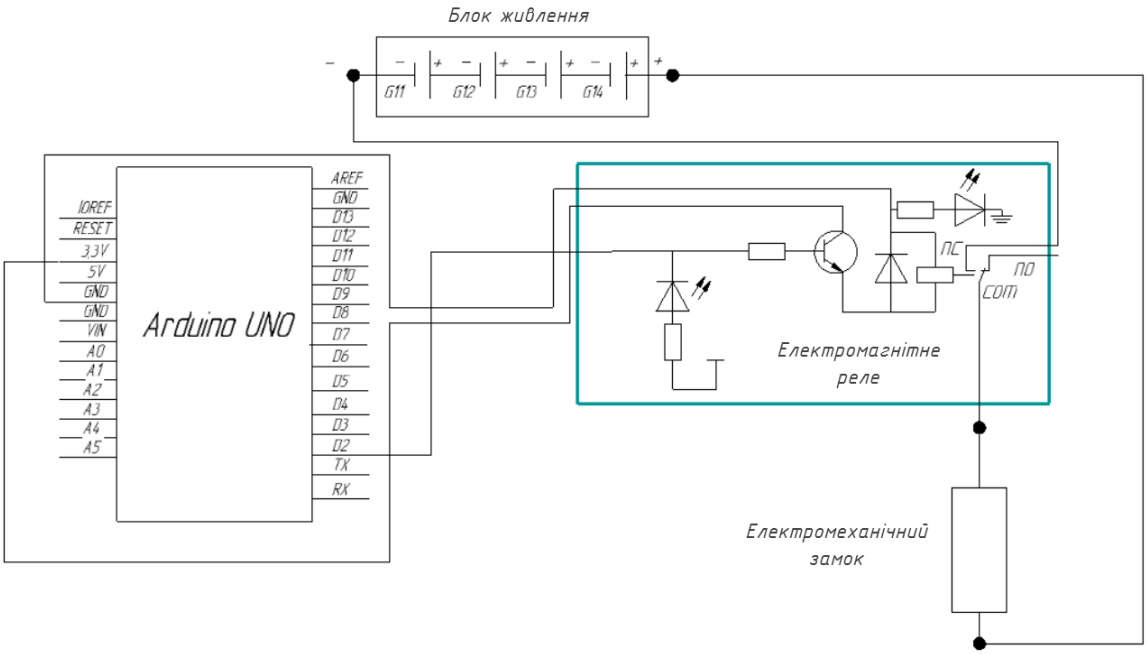

Рисунок 3.8 – Функціональна схема підключення реле

3.3.3. Підключення пристроїв світлового та звукового сповіщення

В якості пристроїв звукового та світлового оповіщення про режим роботи замку в даному проекті використовуються:

– світлодіод зелений *510PG2C* 3В, 20мА;

– світлодіод червоний *510HR3C* 2.6В, 20мА;

– п'єзовипромінювач звуку *HPA17A* 5 5В, 22мА;

– *C1-4* резистор 0,25 Вт, 5%, 150 Ом;

– *C1-4* резистор 0,25 Вт, 5%, 100 Ом.

Так як п'єзовипромінювач звуку *HPA17A* розрахований на напругу 5 В, а саме така напруга на виводах контролера *Arduino UNO*, то даний п'єзовипромінювач підключається до будь-якого виводу контролера виводом + і на висновок *GND* контролера виводом – безпосередньо.

Світлодіоди так підключати не можна, тому що при робочому струмі 20 мА вони в середньому вимагають напругу 2.6-3.3 В, залежно від світлодіода. Тому дані світлодіоди підключаються до виводів контролера кожен через резистор. Червоний світлодіод при струмі 25 мА потребує всередньому 2.6 В. В середньому, так як світлодіод має нелінійну ВАХ, тому у кожного виробника вимоги щодо напруги для кожного виду світлодіодів є різними.

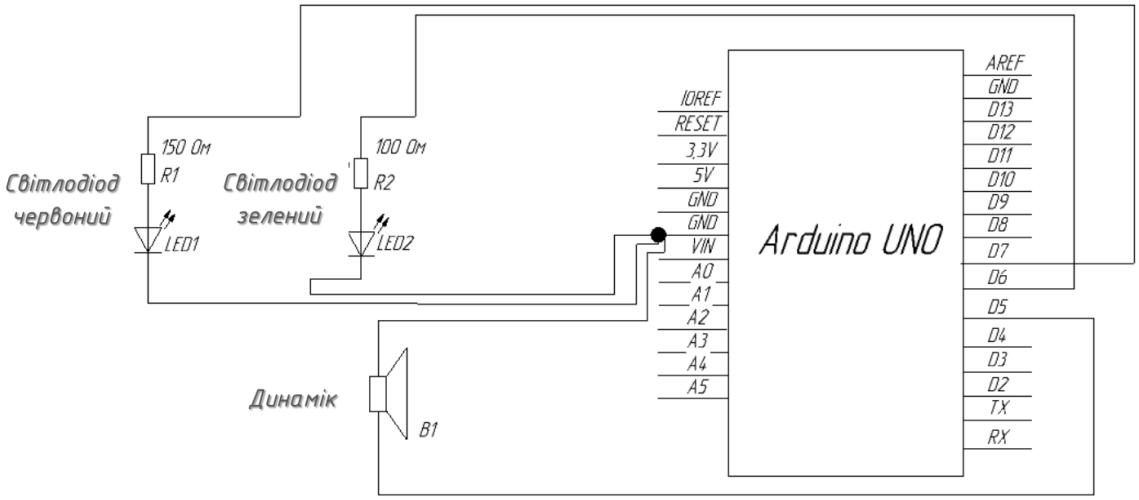

Рисунок 3.9 – Функціональна схема підключення п'єзодинаміка та світлодіодів

Світлодіоди мають по дві ніжки. Одна – коротша, інша довша. Довга ніжка – це анод. Він підключається до виводу контролера, на якому буде висока напруга. Коротка ніжка – катод вона підключається до *GND* контролера. Червоний світлодіод підключається до виводу контролера послідовно через резистор 150 Ом. Зелений вимагає в середньому напруги 3 В. Він підключається

до виводу контролера послідовно через резистор 100 Ом. Принципова схема підключення п'єзодинаміка та світлодіодів показана на рис. 3.9.

3.3.4. Підключення сонячних модулів та блока живлення

Для роботи всієї системи, що розробляється, необхідний якесь джерело живлення. У цьому проекті використовуються 10 сонячних панелей, які мають потужність 10 Вт. Одна сонячна панель може забезпечити рівень напруги 6 В і 160 мА струму. Якщо ми підключимо дві такі панелі послідовно, то ми отримаємо панель, яка може забезпечити 12 В при 160 мА струму. Далі, якщо з'єднати дві панелі по 12 В і 160 мА струму паралельно, ми отримаємо панель, яка забезпечує 12 В напруги і 320 мА струму. Таким чином, якщо з'єднати панелі так як показано на рис. 3.10, то ми отримаємо на виводах сонячної панелі 12 В напруги та приблизно 1 А струму.

Для забезпечення живлення системи, що розробляється, протягом 12 годин роботи темного часу доби потрібно акумулятор, ємністю мінімум 4800 мА/год, що забезпечує 12 В постійної напруги, так як усереднено (залежно від режиму роботи) споживана потужність складає 4Вт та ділиться так:

- *ESP 8266* – 0,825 Вт;
- *Arduino UNO* – 0,48 Вт;
- два світлодіоди і резистори – 0,3 Вт;
- п'єзодинамік – 0,02 -0,96 Вт;
- електромеханічний замок – 0,96.

Для цього необхідно 8 акумуляторів 18650 3.7В, 2600 мА/год. Кожен акумулятор забезпечує напругу 3,7 В. Якщо з'єднати акумулятори послідовно по 4 штуки, (попередньо розрядивши всі акумулятори до 0) то ми отримаємо блок живлення 12 В (*EMS1117* здатний витримати напругу до 18 В) ємністю 2600 мА/год. Отже, нам необхідно з'єднати два таких блоки для отримання блоку живлення 12 В і 5200мА/год, чого більш ніж вистачить для безперебійного живлення нашої системи. Схема підключення показана рис.3.10.

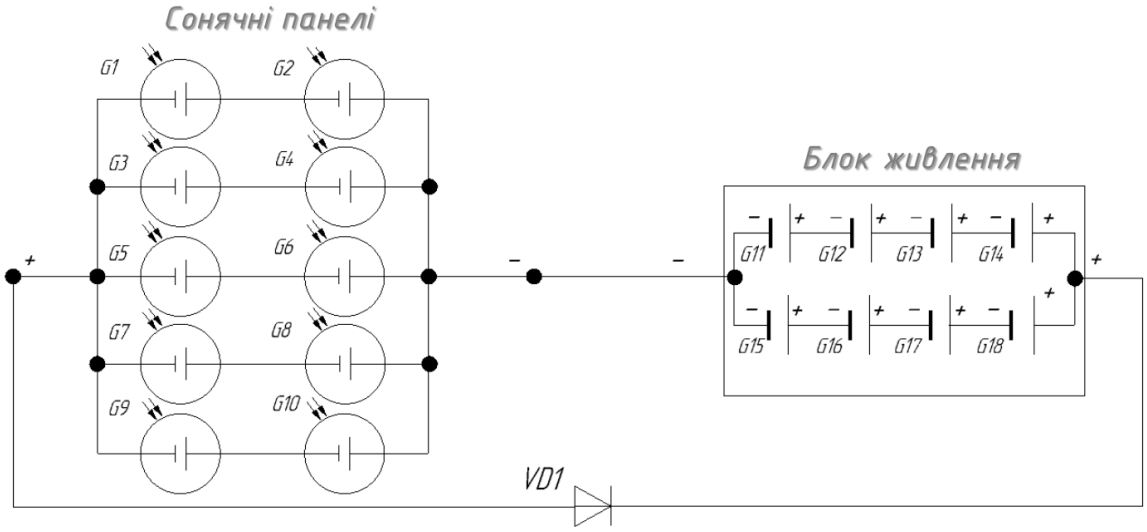

Рисунок 3.10 – Функціональна схема підключення сонячних панелей та блока живлення

Так як можуть бути випадки, коли на сонячних панелях напруга може бути менше 12 В, наприклад, коли панелі погано висвітлюються, то для запобігання руху струму від блоку живлення, до сонячних панелей послідовно з панелями підключимо діод *1N4007* 1А, 1000 В.

3.4. Розробка алгоритму управління для мікроконтролера

Програма, що управляє роботою системи, складатиметься з двох частин:

- створення сервера;
- створення програми, керованої відповіддю сервера на запит клієнта.

Алгоритм роботи системи: користувач, якому потрібно відкрити замок, підключається до точки доступу *Wi-Fi*, яка створюється модулем *Wi-Fi*. Потім користувач вводить пароль (ідентифікатор) і, якщо пароль вірний, користувач підключається до модуля, заходить у браузер телефону за посиланням 192.168.4.1 (*ip* адреса модуля). Далі, замок відкривається і звучить звуковий сигнал. За 5 секунд замок закривається.

Для програмування використовується інтегроване середовище розробки *Arduino – Arduino IDE*.

Управляти модем *ESP8266 01* можна відправлення йому *AT*-команд.

AT-команди – це набір команд, спочатку розроблених 1997 року компанією *Hayes* для своєї продукції. Усі команди *AT* починаються з літер *AT*.

Спочатку необхідно, щоб модуль *Wi-Fi* створив сервер, при зверненні до якого відкривався замок. Для цього спочатку необхідно скористатися наступними командами:

- *AT* (це команда для перевірки модуля. Очікувана відповідь від нього – *OK*.);
- *AT + CWMODE* = 3 (команда для визначення режиму роботи модуля. 1-клієнт, 2- точка доступу, 3- суміщений);
- *AT+RST* (перезавантаження модуля. Необхідно для *CWMODE*);
- *AT+CWSAP = "ARDUINOUNO"*, "123456789",1,4 (налаштування «імені», «пароля», номера каналу та типу шифрування даних);
- *AT+CIPMUX* = 1 (включення режиму множинних підключень);
- *AT+ AT+CIPSERVER* = 1,80 (завдання запуску сервера та порту).

Константа 1 вказує на те, що сервер буде запущено. Порт номер 80 використовується протоколом передачі гіпертексту HTTP. Отже, щоб сервер зареєстрував підключення до нього пристрою користувача, необхідно, щоб користувач скористався браузером телефону і ввести в адресний рядок *IP* сервера. *AT+CIFSR* (відображення *IP*-адреси сервера.)

При підключенні до сервера, модуль відправить на контролер інформацію про пристрій, що підключається.

Подача напруги на реле, та інші пристрої буде здійснюватися у разі, якщо в надісланій від сервера відповіді буде знайдено якийсь певний набір символів. У описаній нижче програмі таким набором символів є слово *Accept*. Але за бажання, можна вказати будь-яку іншу послідовність символів.

Нижче представлені програмні коди з керуючою програмою, написаною в *Arduino IDE.*

Код програми створення сервера:

```
char answer [1500];
void setup ( )
{
Serial.begin (115200); // задання швидкості роботи порту передачі даних
115200
pinMode (5, OUTPUT); // 5 вихід сигналу для електромагнітного реле
pinMode (8, OUTPUT); // 8 вихід для зеленого світлодіоду
pinMode (9, OUTPUT); // 9 вихід для червоного світлодіоду
pinMode (10, OUTPUT); // 10 вихід для п'єзодинаміка
digitalWrite (5, LOW); // установка низького логічного сигналу на виході 5
digitalWrite (8, LOW); // установка низького логічного сигналу на виході 8
digitalWrite (9, HIGH);// установка високого логічного сигналу на виході 9
digitalWrite (10, LOW); //установка низького логічного сигналу на виході 10
Serial.println ("AT"); // відправка команди перевірки готовності модуля по
інтерфейсу UART від контролера до модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+RST"); // відправка команди перезагрузки модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+CWMODE=3"); // відправка команди сумісного режиму роботи
модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+CIPMUX=1"); // відправка команди множинних підключень
delay (2000); // очікування 2 секунди
Serial.println ("AT+CIPSERVER=1,80"); // відправка команди запуска сервера
та використання 80 пора
delay (2000); // очікування 2 секунди
}
void loop ( )
```

Код керування відповіддю сервера на запит клієнта:

```
}
void loop ( )
{
  int i; // ініціалізація змінної i
  if (Serial.available ( ) ) // якщо Arduino отримує які небудь дані,
  починається цикл запису даних у масив
  {
    for (i=1; i<1501-1; ++i) // умови циклу
        {
      if (Serial.available ( ) ) // якщо передачі нема, то вихід з циклу
      break;
      ansver [i] = Serial.read ( ); // запис отриманих даних у кожну комірку
      масива
        }
ansver [i] = 0; // нема даних у масиві
  if (strchr (answer, 'Accept:') !=NULL) // функція пошуку символів Accept
  в масиві answer, якщо знайдені, то виконуються функції нижче
  {
digitalWrite (5, HIGH); // подача високого логічного сигналу на вихід реле
digitalWrite (8, HIGH); // подача високого логічного сигналу на зелений
світлодіод
digitalWrite (9, LOW); // подача низького логічного сигналу на червоний
світлодіод
```

```
tone (10, 15000, 5000); // включення п’єзодинаміка для звук.сигналу частотою 15кГц тривалістю 5 секунд
delay (5000); // очікування 5 секунд
digitalWrite (5, LOW); // подача низького логічного сигналу на вихід реле
digitalWrite (8, LOW); // подача низького логічного сигналу на зелений світлодіод
digitalWrite (9, HIGH); // подача високого логічного сигналу на червоний світлодіод
```

Висновок до третього розділу

У даному розділі обґрунтовані вимоги до проектування, наведено класифікацію методів ідентифікації та обрано метод ідентифікації для даного проекту. Розроблені технічні завдання структурна схема системи управління доступом. Також проведено вибір електронних компонентів та розроблено функціональні схеми: підключення *Wi-Fi* модуля, підключення електромагнітного реле, підключення пристроїв світлового та звукового сповіщення, підключення сонячних модулів та блока живлення. Також розроблено алгоритм управління для мікроконтролера *Arduino UNO* за допомогою програми *Arduino IDE* інтегрованої у середовище. Для отримання доступу користувачеві необхідно за допомогою смартфона підключитися до точки доступу системи і ввести особистий ідентифікатор. Ідентифікатор вірний, система відкриває замок, вмонтований в будь-які двері. Також, про режим роботи системи повідомляє звуковий та світловий сигнали.

РОЗДІЛ 4
ЕКОНОМІЧНІ РОЗРАХУНКИ ПРОЕКТУ

«В умовах відкритої ринкової економіки розширюється діапазон оцінки ефективності науково-технічних розробок, а отже, збільшується кількість основних видів ефективності НДДКР, які необхідно визначити з метою цієї оцінки» [7]. До них належать:

– ***науково-технічний ефект***, який проявляється з впровадженням засобів автоматизації та механізації у виробничі процеси сучасного підприємства, впровадження техніки, що підвищує ефективність виробництва та продуктивність роботи. Техніка, що відповідає за своїми техніко-економічними показниками світового рівня, а також прогресивна технологія та передові методи організації виробництва, які забезпечують підвищення його ефективності. При цьому розрізняють нову техніку, вдосконалену на основі принципів, що вже використовуються, і нову, засновану на останніх досягненнях науки і принципово нових технологіях. Цей захід стимулює науково-технічний ефект;

– ***економічний ефект***, системи контролю доступу мають значний економічний вплив. Сфери застосування системи контролю управління доступу (СКУД) різноманітні: офіси компаній; бізнес-центри; банки; заклади освіти (школи, технікуми, виші); промислові підприємства; охоронювані території; автостоянки, паркування; місця проїзду автотранспорту; приватні будинки, житлові комплекси, котеджі; готелі; громадські установи (спорткомплекси, музеї, метрополітен та ін.). Все це сприяє зростанню бізнесу, розширенню ринків збуту та підвищенню продуктивності, що відображається на загальному економічному розвитку країни;

– ***соціальний ефект***, складаєтьзя з впровадження конролю та забезпечення безпеки на підприємстві або організаціях. Встановлення обладнаного контрольно-пропускного пункту дає змогу значно збільшити

ефект контролю щодо запобігання та несанкціонованого доступу сторонніх на територію об'єкта. Захист матеріальних цінностей об'єкта, а також захист комерційних секретів та прав на інтелектуальну власність дає додатковий економічний ефект. Дані про проходи зберігаються у пам'яті системи та виявляються незамінними під час проведення службових розслідувань. Захист матеріальних цінностей та документів, а також комерційних секретів та прав на інтелектуальну власність можливий також за допомогою встановлення внутрішньої системи охорони приміщення;

– ***маркетинговий ефект***. Саме система контролю та управління доступом (СКУД) є найбільш ефективним засобом моніторингу та управління персоналом. Можна навіть не згадувати про завдання забезпечення специфічних алгоритмів доступу, інтеграцію із суміжними системами безпеки або вбудовування в IT-інфраструктуру з точки використання спільних мереж передачі даних. Набагато важливіше те, що саме СКУД – один з акумуляторів відомостей про персонал і відвідувачів, їхнє місцезнаходження тощо. Ефективно взаємодіючи із системами управління бізнес-процесами, СКУД справді здатна давати економічний ефект. Наприклад, якщо система контролю та управління доступом обмінюється даними із системами техобслуговування та ремонту, управління нарядами, кадровою системою (в якій є інформація про допуски, інструктажі з ТБ тощо), то з'являється можливість оптимізувати кількість персоналу таких служб, оперативно керувати розподілом персоналу між об'єктами обслуговування, правами доступу певного персоналу до об'єктів обслуговування тощо. Серед джерел можливого економічного ефекту від запровадження та використання автоматизованої системи, що підтримує процес контрольно-пропускного режиму можна виділити: зовнішні (захист законних інтересів об'єкта; захист власності об'єкту, її раціональне та ефективне використання; зовнішня стабільність об'єкта; захист комерційних секретів та прав на інтелектуальну власність) та внутрішні (підтримка порядку внутрішнього управління; внутрішня стабільність об'єкта енергонезалежне зберігання списків доступу та списків подій у контролерах; розмежування прав

доступу до приміщень, за часом, за статусом пропуску; захист від передачі пропуску; багаторазовий односторонній прохід; постановка приміщень на системну охорону.

«Науково-технічну ефективність (*НТЕ*) результатів прикладних робіт визначають на основі показників науково-технічного рівня. Оцінка науково-технічної ефективності НДДКР відбувається на основі показника ($О_{НТЕ}$), який представляє собою ступінь досягнення максимально можливого рівня, значення якого дорівнює 1 (одиниці)» [7]:

$$О_{НТЕ} = К^{Ф}_{НТЕ} / К^{П}_{НТЕ}, \quad (4.1)$$

де $К^{Ф}_{НТЕ}$ – показник (коефіцієнт) фактичного рівня науково-технічної ефективності;

$К^{П}_{НТЕ}$ – показник (коефіцієнт) потенціально можливого рівня науково-технічної ефективності (дорівнює одиниці).

Значення показника $К^{Ф}_{НТЕ}$ визначають на основі шкали експертних оцінок (табл. 4.1).

Таблиця 4.1

Шкала експертних оцінок для виміру рівня науково-технічної ефективності проектів

№	Групи показників	Характеристика показників	Інтервал рейтингового числа	Коефіцієнт значущості показників
1	Науково-технічний рівень	Перевищує кращі світові аналоги	10	0,35
		Відповідає світовому рівню	9	
		Нижче кращих світових аналогів	6 – 8	
		Перевищує кращі вітчизняні аналоги	3 – 5	
		Відповідає вітчизняному рівню	1 – 2	
		Нижче вітчизняного рівня	0	

Продовження таблиці 4.1

№	Групи показників	Характеристика показників	Інтервал рейтингового числа	Коефіцієнт значущості показників
2	Перспектив-ність	Першочергова значущість	8 – 10	0,35
		Значущий	5 – 7	
		Корисний	1 – 4	
3	Потенційний масштаб практичного використання	Світовий ринок	10	0,2
		Галузі національної економіки	7 – 9	
		Галузь (регіон)	3 – 6	
		Окремі підприємства (об'єднання)	1 – 2	
4	Ступінь вірогідності досягнення позитивних результатів	Великий	10	0,1
		Середній	5 – 9	
		Малий	1 – 4	

Проведення оцінки

Визначають $K^{Ф}_{НТЕ}$ на основі експертної оцінки науково-технічного рівня розробки.

З цією метою:

− розроблюють перелік специфічних показників, необхідних для виміру науково-технічного рівня розробки;

− формують групу аналогів, які реалізовані на світовому і вітчизняному ринках;

− здійснюють відповідні розрахунки для співставлення показників і визначення балів по табл. 4.1.

До числа специфічних показників відносять:

− **для нової техніки**: «продуктивність, споживання інженерних ресурсів на виробітку одиниці продукції, потреба в робочих, які обслуговують обладнання, експлуатаційні витрати на одиницю продукції» [7];

− **для нових матеріалів і речовин**: матеріали і речовини, використовувані в мережі доступу за допомогою супутникових технологій, мають важливу роль у забезпеченні надійного та ефективного зв'язку. Система контролю та управління доступом включає сукупність організаційних і технічних засобів, за допомогою яких вирішуються завдання управління допуском людей у приміщення різної категорії, зони обмежені в доступі, обліку та контролю. Пропускні пункти, входи/виходи в будівлі та приміщення оснащуються засобами, що забезпечують обмеженість доступу. Дане обладнання підключаються до контролерів системи, які об'єднуються в мережу та підключаються до головного комп'ютера, з якого здійснюється управління та контроль функціонування системи. Оптимальний вибір матеріалів та речовин допомагає забезпечити стабільну та швидку передачу даних в мережі доступу за допомогою супутникових технологій;

− **для нових технологій**: «якість виробленої продукції, енергоємність і трудомісткість продукції, собівартість одиниці продукції» [7].

З метою спрощення визначення $К^{Ф}_{НТЕ}$ у табл. 4.2 не введено показника витрат на одиницю продукції.

Таблиця 4.2

Порівняльні показники для виконання оцінки НТЕ

Показники	Варіанти технології	
	розробленої	співвідносної (аналога)
Рівень новизни	світовий	-
Якість продукції	найвища	вища

Продовження таблиці 4.2

Показники	Варіанти технології	
	розробленої	співвідносної (аналога)
Споживання на 1 т продукції: – тепла, Гкал – електроенергії, кВт·годину – води, $м^3$	 5,14 46,72 4,13	 6,85 54,36 3,12
Трудомісткість виробництва, людино-годин/ тонну	17,5	6,17

На основі співставлення даних таблиці встановлюють бали по характеристиках чотирьох груп і на цій основі розраховують значення інтегрального показника НТЕ:

$$НТЕ = \Sigma Б_i \times К_i^3, \quad (4.2)$$

де $i = 1 \div 4$,

Бі – бали (рейтингове число),

К – коефіцієнт значущості показників.

Рівень науково-технічної ефективності НДДКР розраховано на основі наведених даних прикладу (табл. 4.3).

Таблиця 4.3

Експертна оцінка і розрахунок величини інтегрального показника НТЕ

№	Групи показників	Рейтинг експертів			Середня за експертними оцінками	НТЕ
		1	2	3		
1	Науково-технічний рівень	9	8	7	8	2,8 (8 х 0,35)

Продовження таблиці 4.3

№	Групи показників	Рейтинг експертів			Середня за експертними оцінками	НТЕ
		1	2	3		
2	Перспективність	6	5	5	5,33	1,87 (5,33 х 0,35)
3	Потенційний масштаб практичного використання	7	8	8	7,67	1,53 (7,67 х 0,20)
4	Ступінь вірогідності досягнення позитивних результатів	8	8	7	7,67	0,77 (7,67 х 0,10)
В С Ь О Г О						6,97

НТЕ = 8·0,35+5,33·0,35+7,67·0,20+8·0,10=2,8+1,87+1,53+0,77 = 6,97

Отриманий результат слід порівняти з максимально можливим значенням, яке дорівнює 10 балам (10·0,35 + 10·0,35 + 10·0,20 + 10·0,10).

Отже, оцінка рівня НТЕ може бути зроблена за допомогою інтегрального коефіцієнта оцінки НТЕ ($К_{НТЕ}$):

$$К_{НТЕ} = \frac{НТЕ}{10} \cdot 100\ \%\ . \qquad (4.3)$$

На основі даних табл. 4.3 можно дійти до висновку, що $К_{НТЕ}$ відповідає 69,7 %, тобто:

$$К_{НТЕ} = \frac{6,97}{10} \cdot 100 = 69,7$$

В тому випадку, коли значення $К_{НТЕ}$ перевищує середнє значення, яке дорівнює 5,0, має бути зроблено висновок про достатній рівень НТЕ:

- цілком достатній 5,0 – 6,0;
- достатній 6,1 – 8,0;

- достатньо високий 8,1 – 9,0;
- високий 9,1 – 10.

Таким чином, рівень *HTE* технології можна визнати достатнім. Отже, розроблену технологію пропонується впроваджувати у виробництво.

Визначимо вартість електронних компонентів проектованої СКУД, дані зведемо у таблицю 4.4.

Таблиця 4.4

Вартість матеріалів проектованого приладу

Найменування компоненту	Вартість, грн.
1. *Arduino UNO* на базі процесора *ATmega328*.	380,00
2. *Wi-Fi* модуль *ESP8266-01*.	142,00
3. Електромагнітне реле srd-05vdc-sl-c.	19,00
4. Електромеханічний замок «ATIS Lock G».	855,00
5. Перетворювач напруги AMS1117.	8,00
6. П'єзовипромінювач звуку *HPA17A* 5В, 25мА.	15,00
7. Світлодіод зелений 510PG2C 3В, 20мА.	5,00
8. Світлодіод червоний *510HR3C* 2.6В, 20мА.	5,00
9. С1-4 резистор 0,5 0,25 Вт, 5%, 150 Ом; С1-4 резистор 0,25 Вт, 5%, 220 Ом; С1-4 резистор 0,25 Вт, 5%, 100 Ом.	1,00×3
10. Діод *1N4007* 1А, 1000 В.	1,00
Вартість без урахування безперебійного блоку живлення 1433,00 грн.	
11. Сонячний модуль 6В, 1 Вт– 10 шт.	120,00×10
12. Акумулятори літієві 18650 3.7В, 2600 мАч – 8 шт.	95×8
Вартість всього пристрою 3393 грн.	

Висновки до четвертого розділу

Доцільність створення та впровадження нової техніки в умовах самоокупності та самофінансування областей, об'єднань та підприємств, що її застосовують, залежить від ціни нової техніки. Методи визначення її ефективності повинні відповідати методиці оцінки корисного ефекту нової техніки в споживанні. Відповідно до цієї методики корисний ефект нової техніки у споживанні включає вартісну оцінку споживчих властивостей нової техніки, які впливають на її продуктивність, надійність, тривалість, економічність витрати робочої сили, електроенергії, палива, сировини, матеріалів, виробничих площ та інших ресурсів, якість роботи, соціальні та екологічні показники.

Вартість проектованого приладу без урахування безперебійного блоку живлення становить1433,00 грн. Вартість всього пристрою складає 3393 грн. У порівнянні з електромеханічним замком *Geos Lock* з *GSM* модулем (8180 грн.) можна зробити висновок, що розроблений прилад має не тільки технічні переваги (безперебійне живлення), а й значно нижчу кошторисну вартість.

Розрахований коефіцієнт науково-технічної ефективності становить 69,7 %, тобто рівень НТЕ технології можна визнати достатнім. Отже, розроблену технологію пропонується впроваджувати у виробництво.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

5.1 Основні положення техніки безпеки

Охорона праці – це система законодавчих, організаційно-технічних, соціально-економічних, санітарно-гігієнічних і лікувально-профілактичних мір і засобів, спрямованих на збереження життя, здоров'я й працездатності людини в процесі праці. Об’єктом управління охороною праці є діяльність структурних підрозділів, функціональних служб і всього колективу підприємства по забезпеченню здорових і безпечних умов праці на робочих місцях, виробничих ділянках і підприємстві в цілому. Завдання охорони праці полягає в тому, щоб звести до мінімуму ймовірність поразки працюючого під дією небезпечного виробничого фактору або захворювання під дією шкідливого виробничого фактору з одночасним забезпеченням комфортних умов при максимальній продуктивності праці. Метою виконання даного розділу є проведення аналізу характеристик проектованого об'єкта й умов його роботи.

При роботі з приладом слід дотримуватися загальних правил техніки безпеки поводження з радіо і електроприладами.

Дотримання вимог і виконання правил техніки безпеки, регулярне проведення відповідних заходів сприяє підвищенню продуктивності праці, якості продукції та збереженню здоров'я працюючих.

5.2 Класифікація виробництва за мірою вибуховою, вибухопожежною і пожежною небезпекою

Під охороною праці розуміється система законодавчих актів, організаційних і технічних заходів і засобів, спрямованих на захист і збереження здоров'я і життя людини в процесі праці.

Згідно класифікації виробництв за мірою вибуховою, вибухопожежній і пожежній небезпеці будівлі діляться на: А, Б, В, Г, Д. Приміщення, в яких розміщуються ЕОМ і приміщення, де обслуговуються ЕОМ, відносяться до категорії В – пожежонебезпечні.

Категорія В – пожежонебезпечні виробництва, в яких застосовуються рідини з температурою спалаху >610С і горючий пил з НВП >65г/м3, до цієї категорії відносяться будівлі, в яких розміщуються ЕОМ, і приміщення, де обслуговуються ЕОМ.

Об'ємно-планувальні рішення по розміщенню проектованої установки або пристрою

Організація робочого місця користувача відеотерміналу і ЕОМ повинна забезпечувати відповідність усіх елементів робочого місця і їх розташування ергономічним вимогам.

Площа, виділена для одного робочого місця з відео терміналом або персональною ЕОМ, повинна складати не менше 6 кв.м., а об'єм - не менше 20куб. м

Робоче місце з відео терміналами повинне розташовуються на відстані не менше 1м від стін зі вставними отворами.

Відстань між бічними поверхнями відеотерміналів і екраном має бути менше 1,2 м.

Відстань між тильною поверхнею одного відео терміналу і екраном іншого не менше 2,5 м.

Екран відеотерміналу повинен розташовуватися на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахуванням розміру алфавітно-цифрових знаків і символів.

Класифікація приміщення по мірі небезпеки поразки електричним струмом

Згідно класифікації приміщення, в яких експлуатуються ЕОМ, відносяться до приміщень без підвищеної небезпеки (нормальна температура і вологість, сухі, струмонепровідної підлоги), оскільки це мають бути

приміщення, що відповідають усім вимогам до мікроклімату і з ізолюючими підлогами.

Класифікація устаткування за ПУЭ

Правилами пристрою електроустановок за умовами електробезпеки електроустановки підрозділяється на електроустановки до 1 кВ і електроустановки вище 1 кВ (по діючому значенню напруги). Практика свідчить, що електротравми частіше трапляються в електроустановках до 1000 В.

За способом захисту людини від поразки електричним струмом ЕОМ повинні відповідати першому класу захисту.

Не допускається підключення ПЕВМ до звичайної двопровідної мережі, у тому числі з використанням перехідних пристосувань. Є неприпустимою експлуатація кабелів і дротів з пошкодженою ізоляцією, саморобних подовжувачів.

Захисне заземлення – умисне з'єднання металевих неструмоведучих частин, які можуть виявитися під напругою з штучним заземленням. Застосовується в мережах з напругою до 1000 В з ізольованою нейтраллю, і вище 1000 В з будь-яким режимом нейтралі.

5.3 Пожежна профілактика

Пожежна безпека може бути забезпечена заходами пожежної профілактики і активного пожежного захисту. Поняття пожежної профілактики включає комплекс заходів, необхідних для попередження виникнення пожежі або зменшення його наслідків. Під активним пожежним захистом розуміються заходи, що забезпечують успішну боротьбу з виникаючими пожежами або вибухонебезпечною ситуацією.

Причини пожеж в електроустановках

Велику роль в пожеженебезпекі грає правильний вибір використання електроустаткування.

Система освітлення з лампами розжарювання найбільш небезпечні через те, що температура поверхні колби лампи приблизно дорівнює 500 ºС. Велику роль в безпеці грає правильний вибір типу світильника.

Коротке замикання відбувається у тому випадку, коли точки різних фаз мережі з'єднуються через малий опір. Внаслідок чого миттєво збільшується струм, відбувається виділення великої кількості тепла.

Заходами захисту є: дотримання нормальних режимів експлуатації; своєчасне проведення регламентних робіт; застосування плавких запобіжників і автоматів.

Пожежі в електроустановках відбуваються із-за: короткого замикання, перевантаження мереж, великих перехідних опорів, від електронагрівних приладів.

Засоби пожежної автоматичної сигналізації

Одним з ефективних засобів боротьби з пожежею у виробничому приміщенні є установка системи електричної пожежної сигналізації, яка призначена для:

– виявлення загоряння;

– повідомлення про місце його виникнення;

– ліквідації пожежі.

Основними системами електричної пожежної сигналізації є:

– ізвещателі;

– станція пожежної сигналізації;

– пристрій живлення і лінія зв'язку.

Засоби пожежогасіння

Приміщення з ЕОМ мають бути оснащені переносними вуглекислотними вогнегасниками типу ОУ- 5, призначеними для гасіння загоряння установок напругою до 1000 В, з розрахунку 2 шт. на кожних 20 м2.

У вуглекислотних вогнегасниках застосовують зріджений двоокис вуглецю. Вогнегасільна дія полягає в розбавленні повітря і зниженні в нім вміст кисню до концентрації, при якій припиняється горіння. Вогнегасільний

ефект обумовлюється втратами теплоти на нагрівання двоокису вуглецю і зниженням теплового ефекту реакції. Підходи до засобів пожежогасінні мають бути вільними.

Розрахунок установки пожежогасіння

Це приміщення згідно СНиП 2.04.09-84, відноситься до 1-ої міри вогнестійкості (найнижча небезпека). В даному випадку найбільш доцільним є гасіння пожежі вуглекислотою.

Виробимо розрахунок вуглекислотної установки.

Визначаємо кількість вогнегасільного газового складу Gг :

$$G\text{г} = G\text{в} \cdot V\text{пом} \cdot K\text{уп} \cdot 1{,}25, \text{ кг} \qquad (5.1)$$

де ·*К*уп – коефіцієнт участі, що враховує особливості газообміну і витоку вуглекислоти через нещільність. Зазвичай Куп = $1 \div 2$. Приймемо Куп = 1,0;

*G*в·= 0,7 – вогнегасільна концентрація для вуглекислоти;

*V*пом = 294 м^3 – об'єм приміщення.

$$G\text{г} = 0{,}7 \cdot 294 \cdot 1 \cdot 1{,}25 = 257{,}25 \text{ кг}$$

Визначаємо необхідне число робочих балонів:

$$N_{\text{бал}} = \frac{G_{\text{г}}}{V_{\text{б}} \cdot \rho \cdot \alpha_{\text{н}}} \qquad (5.2)$$

де $V_{\text{б}}$ = 25 літрів – місткість балона;

ρ = 0,625 кг/л – щільність вуглекислоти;

$\alpha_{\text{н}}$ =1 – коефіцієнт наповнення балона.

$$N_{\text{бал}} = \frac{257{,}25}{25 \cdot 0{,}625 \cdot 1} = 16{,}5$$

Приймаємо *N*б = 17 балонів.

Згідно СНиП 2.04.09-84 у складі установки газової пожежогасінні окрім розрахункового має бути стовідсотковий резервний запас вогнегасної речовини. Тому загальну кількість сорокалітрових балонів приймаємо 28 балонів.

5.4 Виробнича санітарія

Виробнича санітарія – система організаційних, технічних засобів, що запобіжать або зменшують дію шкідливих виробничих чинників.

Вимоги до режимів роботи і відпочинку при роботі з ВДТ ЕОМ

Режим праці і відпочинку, що працюють з ЕОМ визначається залежно від виконуваної роботи. Для оператора ЕОМ при 8-ми годинному робочому дні передбачена перерва 10 хвилин через кожних 2 години роботи (для роботи 1 категорії складності). Тривалість безперервної роботи з відеотерміналом без регламентованої перерви не повинна перевищувати двох годин. При роботі в нічну зміну незалежно від категорії виконуваних робіт тривалість регламентованих перерв повинна збільшитися на 60 хвилин. Залучення жінок до робіт в нічний час є неприпустимим.

Психофізіологічні небезпечні і шкідливі чинники

У сучасних високомеханізованих, автоматизованих виробництвах робота вимагає значної нервово-психічної і розумової напруги. На відміну від фізичної напруги воно не проявляється зміною фізіологічних функцій серцево-судинної, дихальної, терморегуляторної і інших систем. Воно торкається головним чином найвищого, координуючого органу – центральної нервової системи. Працездатність розумового або близького до нього по характеру праці залежить від тих же чинників, що і при фізичній праці: загального пристосування функцій головного мозку до розумової роботи, тренованості і вправи, емоційного стану і стану зовнішнього середовища. Причому, емоційний стан при розумовій праці грає велику роль, чим при фізичному.

Долікарська допомога

Найбільш типовими нещасними випадками при роботі з ЕОМ являються нещасні випадки від електричного струму. Перша долікарська допомога людині, ураженій електричним струмом, складається з 2-х етапів:

1. Звільнення постраждалого від дії струму.

2. Надання медичної допомоги потерпілому. Заходи першої медичної допомоги потерпілому залежать від його стану:

– якщо потерпілий у свідомості, але до цього був в непритомності або тривалий час знаходився під струмом, йому необхідно забезпечити повний спокій до прибуття лікаря;

– за відсутності свідомості, але диханні, що збереглося, і роботі серця треба рівно і зручно укласти потерпілого на м'яку підстилку, розстебнути пояс і одяг, забезпечити приплив свіжого повітря. Слід давати нюхати нашатирний спирт, окропляти особу холодною водою, розтирати і зігрівати тіло;

– якщо потерпілий погано дихає – рідко, судорожно або якщо дихання поступово погіршується, необхідно робити штучне дихання методом «з рота в рот'»;

– за відсутності ознак життя потрібно робити штучне дихання і зовнішній масаж серця до появи ознак життя або до прибуття лікаря.

Висновок до п’ятого розділу

У цьому розділі дипломного проекту надана класифікація виробництва за мірою вибуховою, вибухопожежною і пожежною небезпекою. Розроблені заходи по запобіганню від поразки електричним струмом. Розглянуті заходи по наданню долікарської допомоги. Вироблений розрахунок засобів при пожежогасінні, на випадок виникнення пожежі. Також були розглянуті вимоги до робочого місця для роботи з відео терміналом або персональною ЕОМ.

ЗАГАЛЬНІ ВИСНОВКИ

Застосування систем контролю та управління доступом – це один із підходів для забезпечення безпеки окремо взятого об'єкта. Найбільш популярною сферою інтеграції СКУД з функцією моніторингу та управління є використання даної технології у розробці «розумного будинку».

У роботі наведено аналіз систем контролю управління доступом, пристроїв ідентифікації санкціонованого доступу (парольні, біометричні, майнові) та вимог до систем контролю управління доступом: вимоги до технічного та програмного забезпечення, взаємозв'язок з пов'язаними системами, перспективи розвитку та модернізації, надійність, безпечність та гарантоване збереження інформації.

Виходячи з поставлених задач було прийняте рішення розробляти систему контролю доступу на платформі *Arduino* з підтримкою бездротового зв'язку *Wi-Fi.* У проекті розроблені технічні завдання та структурна схема системи управління доступом. Також проведено вибір електронних компонентів та розроблено функціональні схеми: підключення *Wi-Fi* модуля, підключення електромагнітного реле, підключення пристроїв світлового та звукового сповіщення, підключення сонячних модулів та блока живлення. Також розроблено алгоритм управління для мікроконтролера *Arduino UNO* за допомогою програми *Arduino IDE* інтегрованої у середовище. До переваг вибраного методу проектування слід віднести можливість удосконалення системи за рахунок підключення розумних датчиків та алгоритмів, які забезпечуватимуть додаткову безпеку.

Проведені економічні розрахунки з яких можна зробити висновок, що розроблений прилад має не тільки технічні переваги, а й значно нижчу кошторисну вартість. Отже, розроблену технологію пропонується впроваджувати у виробництво.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Б. Ю. Жураковський, І.О. Зенів. Технології інтернту речей. Київ. КПІ ім. Ігоря Сікорського, 2021. – 271 с.

2. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2015. – 492 с.

3. *Richard E. Smith – Authentication: From Passwords to Public Keys 1st Edition.* 2001.

4. *Simon Monk, Programming Arduino, P.*176 (2011).

5. *Ulli Sommer, Arduino, P.*115 (2012).

6. *Jeremy Blum, Exploring Arduino, P.*384 (2013).

7. Методичні вказівки до оцінки науково-технічної ефективності розробки нової технології, нового обладнання та інших інновацій. Для студентів всіх спеціальностей СВО «бакалавр» і «магістр» денної і заочної форм навчання. Укладачі Басюркіна Н.Й., Свистун Т.В. Одеса: ОНТУ, 2022р. 18 с.

8. Системи контролю доступу СКД/СКУД [Електронний ресурс]. – Режим доступу:https://ukrinfosystems.com.ua/uk/design-and-construction/access-control-systems.

9. *Arduino UNO R3*. [Електронний ресурс]. – 2022. – Режим доступу: https://docs.arduino.cc/resources/datasheets/A000066-datasheet.pdf.

10. *Arduino IDE*. [Електронний ресурс]. – 2022. – Режим доступу: https://www.arduino.cc/en/software.

11. Законодавство України про охорону праці [Електронний ресурс]. – 2023.– Режим доступу: https://education.profiteh.kiev.ua/mod/page/view.php?id=66

ДОДАТКИ

Додаток А. Код програми створення сервера

```
char answer [1500];
void setup ( )
{
Serial.begin (115200); // задання швидкості роботи порту передачі даних 115200
pinMode (5, OUTPUT); // 5 вихід сигналу для електромагнітного реле
pinMode (8, OUTPUT); // 8 вихід для зеленого світлодіоду
pinMode (9, OUTPUT); // 9 вихід для червоного світлодіоду
pinMode (10, OUTPUT); // 10 вихід для п'єзодинаміка
digitalWrite (5, LOW); // установка низького логічного сигналу на виході 5
digitalWrite (8, LOW); // установка низького логічного сигналу на виході 8
digitalWrite (9, HIGH);// установка високого логічного сигналу на виході 9
digitalWrite (10, LOW); //установка низького логічного сигналу на виході 10
Serial.println ("AT"); // відправка команди перевірки готовності модуля по
інтерфейсу UART від контролера до модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+RST"); // відправка команди перезагрузки модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+CWMODE=3"); // відправка команди сумісного режиму роботи
модуля
delay (2000); // очікування 2 секунди
Serial.println ("AT+CIPMUX=1"); // відправка команди множинних підключень
delay (2000); // очікування 2 секунди
Serial.println ("AT+CIPSERVER=1,80"); // відправка команди запуска сервера та
використання 80 пора
delay (2000); // очікування 2 секунди
}
void loop ( )
```

Додаток Б. Код керування відповіддю сервера на запит клієнта

```
}
void loop ( )
{
  int i; // ініціалізація змінної i
  if (Serial.available ( ) ) // якщо Arduino отримує які небудь дані, починається
  цикл запису даних у масив
  {
    for (i=1; i<1501-1; ++i) // умови циклу
        {
      if (Serial.available ( ) ) // якщо передачі нема, то вихід з циклу
```

```
      break;
      answer [i] = Serial.read ( ); // запис отриманих даних у кожну комірку
      масива
        }
ansver [i] = 0; // нема даних у масиві
  if (strchr (answer, 'Accept:') !=NULL) // функція пошуку символів Accept в
  масиві answer, якщо знайдені, то виконуються функції нижче
  {
digitalWrite (5, HIGH); // подача високого логічного сигналу на вихід реле
digitalWrite (8, HIGH); // подача високого логічного сигналу на зелений
світлодіод
digitalWrite (9, LOW); // подача низького логічного сигналу на червоний
світлодіод
tone (10, 15000, 5000); // включення п'єзодинаміка для звук.сигналу частотою
15кГц тривалістю 5 секунд
delay (5000); // очікування 5 секунд
digitalWrite (5, LOW); // подача низького логічного сигналу на вихід реле
digitalWrite (8, LOW); // подача низького логічного сигналу на зелений
світлодіод
digitalWrite (9, HIGH); // подача високого логічного сигналу на червоний
світлодіод
```

Додаток В. Графічний матеріал

Рисунок В.1 – Слайд №1

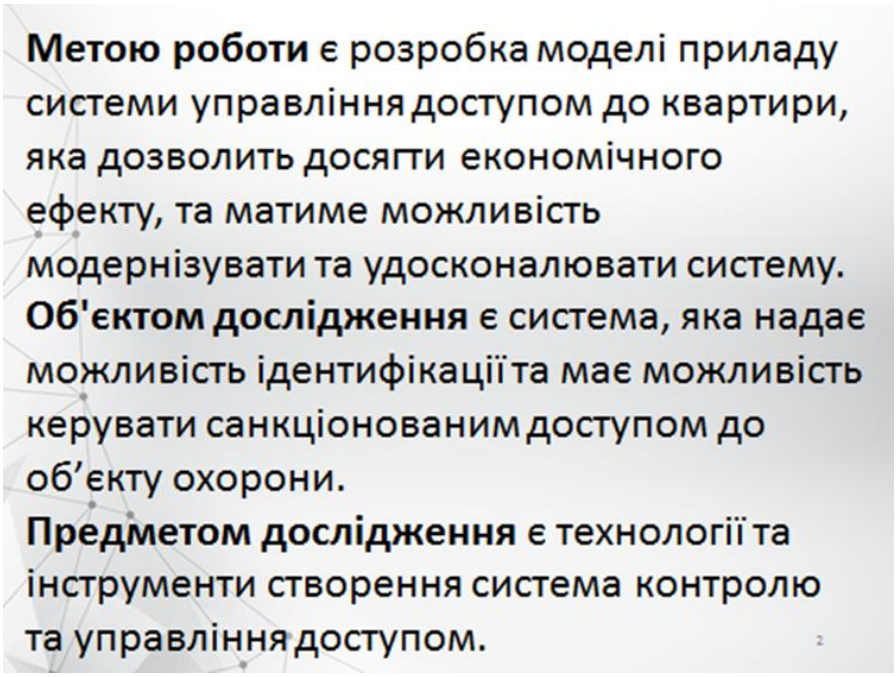

Рисунок В.2 – Слайд №2

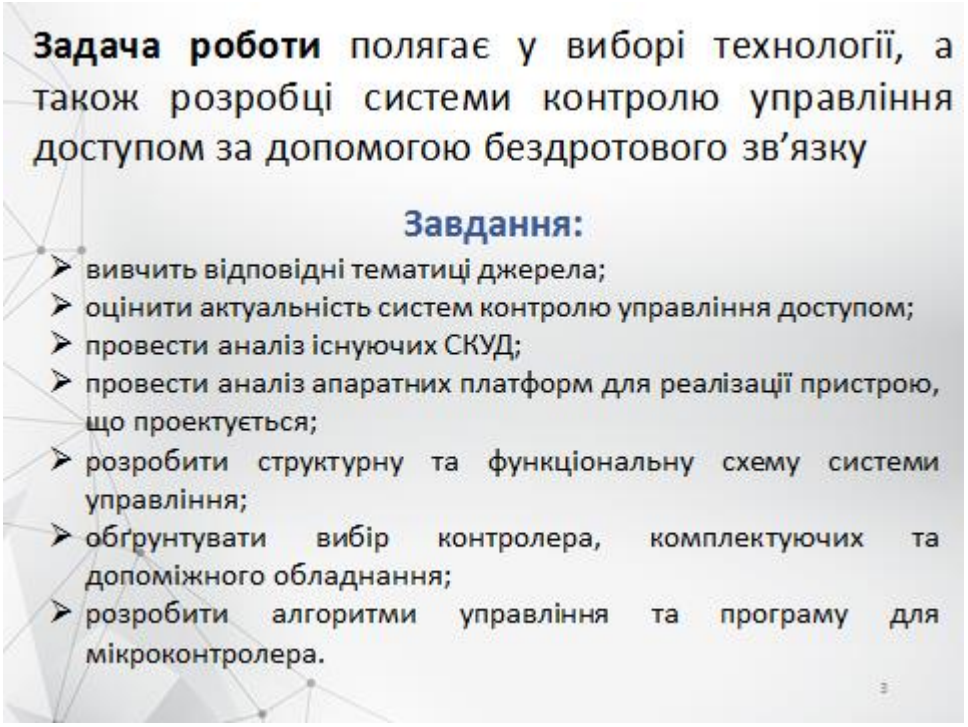

Рисунок В.3 – Слайд №3

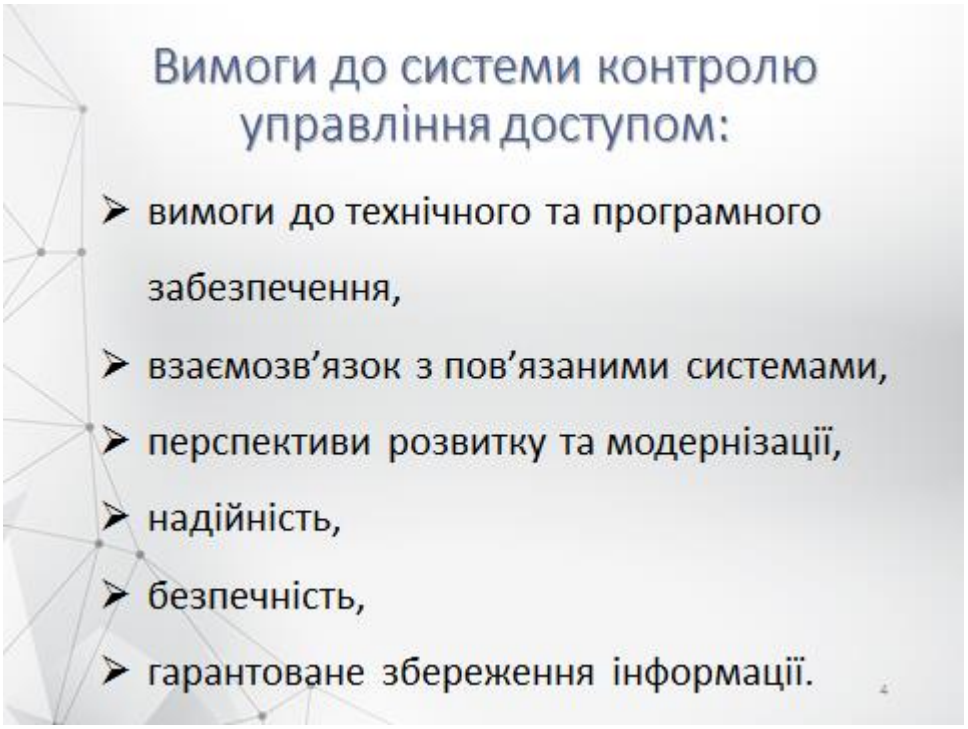

Рисунок В.4 – Слайд №4

Рисунок В.5 – Слайд №5

Рисунок В.6 – Слайд №6

Рисунок В.7 – Слайд №7

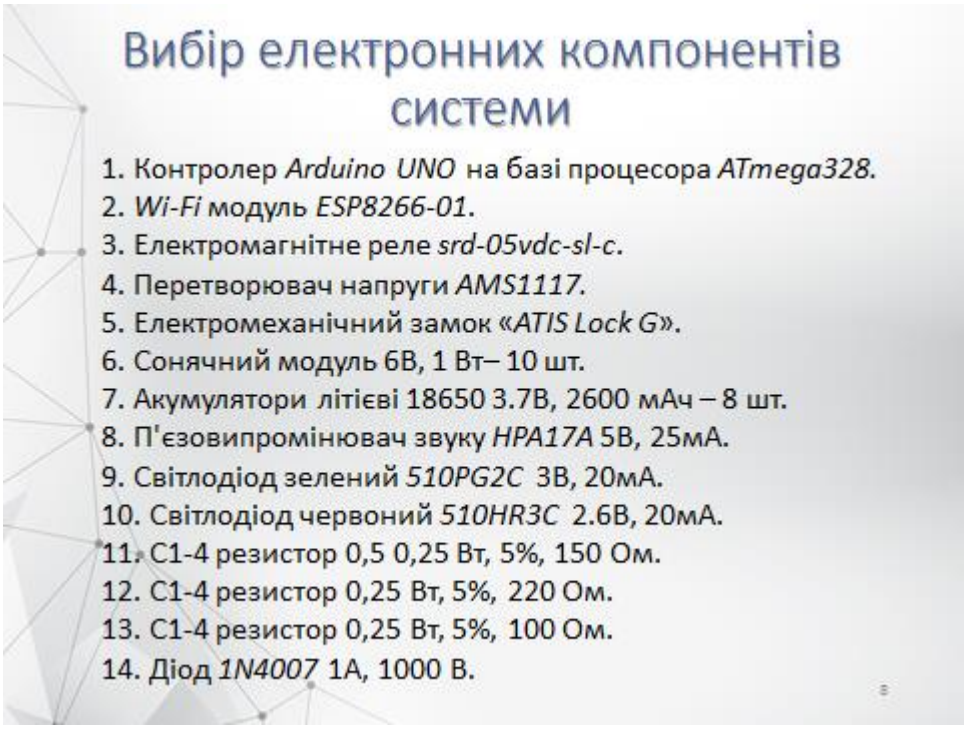

Рисунок В.8 – Слайд №8

Рисунок В.9 – Слайд №9

Рисунок В.10 – Слайд №10

Рисунок В.11 – Слайд №11

Рисунок В.12 – Слайд №12