DOI 10.31891/2307-5732-2024-331-44
УДК 004.056

КОРЧИНСЬКИЙ ВОЛОДИМИР
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
ТАРАСЕНКО ІРИНА
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0009-5736-5979
e-mail: tarasenkoirina1967@gmail.com
РАЦИБОРИНСЬКИЙ СЕРГІЙ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0000-2513-8442
e-mail: raciborinskij@ukr.net
АКАЄВ ОЛЕКСАНДР
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0008-4336-2331
e-mail: dobrodeetel@gmail.com
ХАДЖИОГЛО АРТЕМ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0008-1525-0535
e-mail: artemtemtemtem16@gmail.com

АВТОМАТИЗОВАНІ СИСТЕМИ КЕРУВАННЯ ДОСТУПОМ

У роботі надано огляд та аналіз проблем із застосування автоматизованих систем керування доступом на основі NFC. Досліджено можливості платформи Arduino та на її основі розроблена система керування доступом із модулем RFID-NFC. Використання автоматизованих систем керування доступом у сучасному світі стає все більш актуальним. Це пов'язано з рядом переваг, які такі системи можуть принести підприємствам та іншим об'єктам. Дані системи спрощують і пришвидшують процес ідентифікації особи, заощаджують час та підвищують ефективність роботи служб безпеки, але все одно вимагають контролю з боку людини. Технологія RFID-NFC є актуальною, тому розробка та використання цієї технології для системи керування доступом може вирішити проблеми несанкціонованого доступу до приміщень та/або контрольованих зон. Також компанія/підприємство має змогу заощадити кошти на пристроях ідентифікації, оскільки в якості ідентифікатора можна використовувати різні документи, у яких вбудовано NFC мітку. Наприклад, це може бути паспорт громадянина України, паспорт громадянина України для виїзду за кордон, свідоцтво про реєстрацію транспортного засобу, банківські карти та смартфон із функцією NFC тощо. Автоматизована система керування доступом – це сукупність новітніх технологій та програмного забезпечення, яка призначена для контролю та обмеження доступу до певної приватної території/контрольованої зони. Головною метою автоматизованої системи керування доступом є забезпечення безпеки, управління та моніторингу доступу по приватної території/контрольованої зони. Такі системи використовуються для ідентифікації персоналу, транспортних засобів тощо, які мають доступ до обмеженої території/контрольованої зони. Системи керування доступом можуть бути інтегровані з іншими системами безпеки, як-от: системи відеоспостережень, системи виявлення/запобігання вторгненням тощо.

Ключові слова: Arduino, NFC-мітка, автоматизована система керування доступом, ідентифікація, контрольована зона, системи безпеки, скетч.

KORCHYNSKYI VOLODYMYR, TARASENKO IRYNA, RATSYBORYNSKYI SERHII,
AKAIEV OLEKSANDR, KHADZHYOHLO ARTEM
State University of Intellectual Technologies and Communications

AUTOMATED ACCESS CONTROL SYSTEMS

The paper provides an overview and analysis of the problems in the application of automated access control systems based on NFC. The capabilities of the Arduino platform are investigated and an access control system with an RFID-NFC module is developed on its basis. The use of automated access control systems in the modern world is becoming increasingly relevant. It involves a number of benefits that such systems can bring to businesses and other entities. These systems simplify and speed up the process of identifying a person, save time and increase the efficiency of security services, but still require human control. RFID-NFC technology is up-to-date, so the development and use of this technology for an access control system can solve the problem of unauthorized access to premises and/or controlled areas. Also, a company/enterprise can save money on identification devices, since various documents with an embedded NFC tag can be used as an identifier. For example, it can be a passport of a citizen of Ukraine, a passport of a citizen of Ukraine for travelling abroad, a certificate of registration, bank cards and a smartphone with NFC function, etc. An automated access control system is a set of advanced technologies and software designed to control and restrict access to a specific private territory/controlled area. The main purpose of an automated access control system is to ensure security, control and monitoring of access to a private territory/controlled area. Such systems are used to identify personnel, vehicles, etc. that have access to a restricted area/controlled zone. Access control systems can be integrated with other security systems, such as video surveillance systems, intrusion detection/prevention systems, etc.

Keywords: Arduino, NFC tag, automated access control system, identification, controlled area, security systems, sketch.

Постановка проблеми

Основною задачею автоматизованих систем керування доступом є обмеження доступу людей або працівників підприємства на певний об'єкт до моменту підтвердження прав доступу до нього за допомогою відповідних механізмів та/або електронних пристроїв ідентифікації та аутентифікації. Система контролю доступом дає можливість здійснювати цілодобовий контроль ситуації та території/об'єкті, яка охороняється, забезпечити безпеку співробітників, обмежити несанкціонований доступ до матеріальних цінностей та документів на об'єкті/підприємстві, які мають певний гриф секретності відповідно до законодавства [1].

Загалом усі автоматизовані системи контролю доступу функціонують за схожими принципами, різниця полягає у надійності, якості та зручності повсякденного використання. Також варто відзначити, що система керування доступом складається з [2]:

– ідентифікатора користувача, яким може бути електронний пристрій, карта та навіть людський орган. Якщо це електронний пристрій, то, як правило, всередині нього розміщено чіп із антеною або магнітна смуга. Якщо це людський орган, то в основному використовують відбиток пальця/пальців, відбиток усієї руки, рисунок райдужної оболонки ока або інші біометричні ознаки особистості: риси обличчя, геометрія кісті руки, розміщення вен на руці, динамічні характеристики почерку, особливості мови, динаміка удару по клавішам при друкуванні тощо. Усім ідентифікаторам присвоюється унікальний цифровий код, який містить необхідну інформацію про права доступу його власника;

– зчитувача – це пристрій, який виконує зчитування інформації з ідентифікатора користувача та надсилає отриманні дані у контролер системи доступу;

– загороджувального пристрою (точка проходу) – це турнікети, двері з автоматичними замками, ворота, шлагбауми, шлюзи тощо. Як правило, для повного контролю доступу в точках проходу встановлюють два зчитувачі: один на вході, інший на виході. У випадку, коли потрібен лише вхідний контроль, зчитувач на виході не ставиться, а вхід робиться або вільним, або через спеціальну кнопку виходу;

– кнопки виходу, яка призначена для короткочасного дозволу проходу, при цьому контролер системи доступу запам'ятовує факт виходу через точку проходу;

– контролеру системи контролю доступу – це ключовий електронний модуль, який реалізує ідентифікацію об'єктів доступу за отриманою інформацією від зчитувачів. Також контролер здійснює керування із розмежування доступу на територію, керує загороджувальними пристроями та пристроями оповіщення;

– програмного забезпечення системи керування доступом – це елемент системи, за допомогою якого є можливість централізовано керувати контролерами системи керування доступом, використовуючи персональний комп'ютер, вести моніторинг подій, формувати відповідні звіти тощо;

– конверторів середовища для підключення модулів системи керування доступом одне до одного та до персонального комп'ютера, які надають можливість організувати контроль доступу та облік робочого часу на підприємстві з декількома прохідними, великою кількістю контрольованих зон тощо;

– допоміжного обладнання – це технічні засоби, які застосовуються для забезпечення коректної взаємодії між описаними вище елементами системи керування доступом. До них відносяться конвертори сигналів, блоки живлення, датчики, кнопки, блоки безперебійного живлення тощо.

Подальше вдосконалення систем керування доступом можливе при застосуванні більш ефективних засобів ідентифікації та алгоритмів. Авторами роботи [1] встановлено, що предметом захисту в будь-якій інформаційній системі є конфіденційна інформація. Для запобігання витоку інформації з ЕОМ, окрім програмних засобів захисту інформації, використовуються також і фізичні. Найпоширенішим засобом фізичного захисту інформації є використання системи керування доступом (СКД), яка обмежує доступ до ЕОМ, на якій обробляється ІзОД, особам, які не мають допуску до неї.

Аналіз останніх джерел

У роботі [2] наведено дані про переваги та недоліки СКД на основі радіочастотного доступу. Результати аналізу довели доцільність застосування фізичного захисту ЕОМ, які обробляють інформацію з обмеженим доступом. Більш надійний та зручний захист надає система керування доступом на основі RFID/NFC. Як правило, до захисту конфіденційної інформації ставлять високі вимоги, оскільки крадіжка ІзОД стає загальносвітовою проблемою. Для функціонування інформаційної системи найважливішим завданням є забезпечення надійного та стійкого захисту її від злому. Система керування доступом стає дедалі затребуваною, оскільки все більше компаній захищають свої об'єкти, дані та персонал.

Перші ідентифікатори [2] для систем керування доступом з'явилися у 1980-х роках, які розроблялися на основі карток з магнітними смугами. Використання таких карток дало змогу покращити управління доступом до контрольованих зон, а також вирішити проблему деактивації ключів з бази даних у разі звільнення працівників. У цій технології сканування картки відбувалося шляхом проведення її через спеціальний паз зчитувача для отримання незашифрованих ідентифікаційних даних [2]. Проте через деякий час виявилися недоліки контактної технології [3]. Необхідність фізичного контакту призводило до швидкого пошкодження та зносу магнітного покриття картки, що підвищували витрати на таку СКД. При всіх вказаних недоліках поява та подальший розвиток безконтактних технологій став великим досягненням у історії СКД. На той час найбільш розповсюджена технологія мала назву Prox. Ця технологія використовувала радіочастотний доступ та мала певні переваги перед системою ідентифікації на основі контактного сканування. Зчитування даних карток відбувалось на відстані декількох сантиметрів за допомогою

радіочастотного каналу.

У 2000-х роках відбувся технологічний прогрес створення безконтактних карт. Такі смарт-карти працювали на частоті 13,56 МГц і вже мали певні криптографічні заходи безпеки. По-перше, було реалізовано взаємну аутентифікацію, по-друге, ці карти мали можливість зберігати набагато більше інформації, окрім ідентифікаційного номеру. Усе це дозволило підвищити рівень безпеки та розширити сферу використання даних карт у різних СКД.

Метою роботи є аналіз та розробка алгоритму системи керування на основі радіочастотного доступу із використанням компонентів платформи Arduino.

Виклад основного матеріалу

В залежності від вимог до забезпечення рівня захисту приміщень/контрольованих зон підприємства, реалізована система керування доступом може мати різні рівні складності, що стосуються її архітектури. Для сучасних систем керування доступом може бути виконана класифікація на підставах декількох різних критеріїв. Так, у залежності від метода керування системою, системи керування доступом класифікують як наступні види [4–6]:

– автономні системи керування доступом, які представляють собою самостійні пристрої, що розміщуються в одній точці проходу. Це об'єднання зчитувача та електромагнітного замка в одному корпусі. Такі системи мають обмежену пам'ять на кількість збережених ідентифікаторів і часто не мають функціоналу з ведення журналу виникаючих подій. Такі системи керування доступом застосовуються для захисту окремих приміщень чи входу в будівлю;

– мережеві системи керування доступом є класичними системами керування доступом. Вони призначені для організації комплексного захисту, оскільки мають у собі цілий набір різноманітних зчитувачів та електромагнітних замків, які об'єднані мережевим підключенням із серверною платформою, на яку встановлено спеціальне програмне забезпечення, що дає можливість керувати системою;

– біометричні системи керування доступом є найбільш сучасними, технологічними та безпечними, але вони не сильно розповсюджені через їх високу вартість та складність налаштувань.

У залежності від ключового ідентифікатора, який використовується, системи керування доступом класифікуються наступним чином [6, 7]:

– безконтактні, де використовуються Proxmity-карти або карти з нанесеним на них штрих-кодом. Подібний варіант реалізації зчитувачів у системах керування доступом можна назвати найбільш зручним для користувачів через те, що карти при зчитуванні не прикладаються до зчитувача;

– контактні – це системи керування доступом, де в якості ключа доступу використовуються магнітні карти або «пігулки» у форматі touch-memory брелка із вбудованим чіпом запам'ятовуючого пристрою.

Також існує окрема класифікація систем керування доступом, згідно якої вони поділяються на 4 класи [6]:

– Клас I – це найпростіші системи, до яких входять звичайний електромагнітний замок із замикаючим пристроєм. Системи такого класу мають мінімальний функціонал, а процес ідентифікації співробітників супроводжується звуковими та/або світловими сигналами.

– Клас II – це однорівневі або багаторівневі системи керування доступом, де права відвідувачів можуть налаштовуватись як на підставі виданих їм ідентифікаторів, так і на підставах різних часових рамок. Такі системи можуть функціонувати як автономно, так і безпосередньо через локальні обчислювальні мережі. Як правило, весь час система функціонує через мережу, а в автономний режим переходить автоматично у випадках втрати зв'язку або перебоях/відключенні електроживлення.

– Класи III та IV – це висококласні системи керування доступом, які, окрім контролю, реалізують функціональні можливості з обліку робочого часу, можуть інтегруватися з системами відеоспостереження і охоронно-пожежною сигналізацією, використовують складні ідентифікатори, а також мають багаторівневу взаємодію.

Для усіх сучасних систем керування доступом існують наступні вимоги [7]:

– забезпечувати контроль доступу на усіх типах КПП;

– виключати можливість пронесення/провезення заборонених предметів і препаратів;

– затримувати потенційних порушників як внутрішнього трудового розпорядку, так і зовнішніх відвідувачів, які намагаються проникнути на об'єкти, які знаходяться під охороною.

– мати можливість використовувати різні способи ідентифікації особистості;

– мати відкриту програмно-апаратну платформу, яку в подальшому можна буде інтегрувати з будь-якими іншими системами безпеки;

– забезпечувати автоматизацію процесів управління та координацію діяльності об'єкту;

– системно функціонувати в разі виходу з ладу окремих компонентів та в інших надзвичайних випадках.

Ідентифікація [7, 8] – це надання об'єктам доступу певного ідентифікатора або порівняння наданого ідентифікатора з існуючими, які записано в базах даних систем керування доступом. Існує три види ідентифікації: парольна, апаратна та біометрична. Охарактеризуємо кожну з них [8]:

– парольна ідентифікація ґрунтується на введенні користувачем унікального логіна та пароля для доступу до системи. Користувач отримує персональний логін та пароль, які надають йому доступ до об'єкту

чи системи. Перевагами такої ідентифікації є простота використання та розповсюдженість, а недоліками – залежність від якості обраних паролів та вразливість до атак, які пов'язані з перехопленням паролів;

– апаратна ідентифікація базується на визначенні особистості за предметами власності, такими як: електронні ключі, банківські карти тощо. Її перевагами є висока надійність, оскільки ключі мають певні механізми захисту, а недоліками – висока вартість такого обладнання;

– біометрична ідентифікація виконується за унікальними ознаками, такими як: відбитки пальців, райдужна оболонка ока, рисунок вен на руці тощо. Перевагою такої системи ідентифікації є надійність, а недоліком – висока вартість, оскільки потрібні сканери біометричних параметрів для кожного комп'ютера.

У технології RFID-NFC принцип обміну даними засновано на індуктивному зв'язку між пристроями на відстані до 10 см зі швидкістю передавання до 424 кбіт/с та частотному діапазоні з центральною частотою 13,56 МГц [9]. Технологія NFC заснована на стандартах ISO/IEC 14443A та ISO/IEC 14443B. Для обміну даними між двома NFC-пристроями використовується протокол передавання даними, який відповідає стандартам ECMA-340 та ISO/IEC 18092. Схема передавання даних між опитувальним та приймальним пристроями представлена на рис. 1.

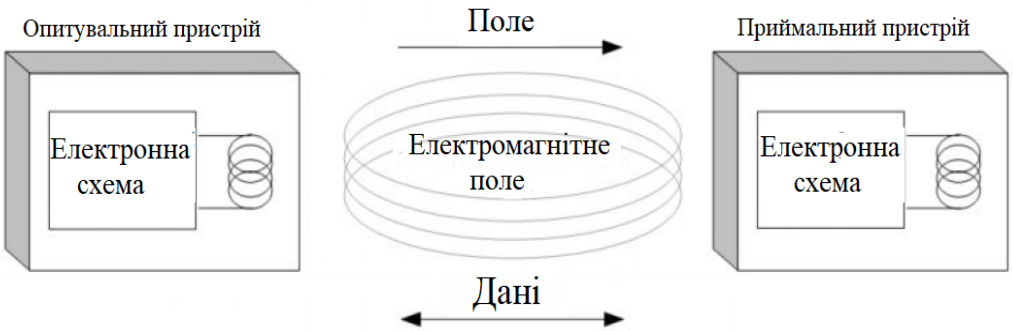

Рис. 1. Схема взаємодії опитувального та приймального пристроїв

Технологія NFC використовує способи цифрового кодування, які представлено на рис. 2:

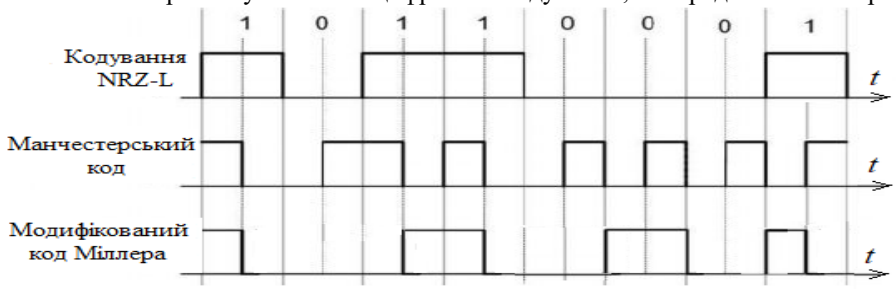

Рис. 2. Способи цифрового кодування у технології RFID-NFC

– метод кодування NRZ-L – високий рівень напруги сигналу на інтервалі часу біта передає логічну «1», а низький рівень напруги сигналу на інтервалі часу біта передає логічний «0».

– манчестерський код – перша половина бітового часового інтервалу логічної «1» передається високим рівнем напруги, а друга половина – низьким рівнем. Логічний «0» передається послідовністю високого на низького рівнів напруги.

– модифікований код Міллера (MFM) – у цьому випадку зміна рівня напруги відбувається в середині такту, якщо біт, що передається, дорівнює логічній «1», і на межі інтервалу, якщо обидва сусідніх біта дорівнюють «0».

Розглянемо переваги системи керування доступом на основі RFID-NFC [9, 10]. Доступ на основі RFID-NFC дає змогу використовувати як мінімум власний смартфон, паспорт громадянина України, свідоцтво про реєстрацію транспортного засобу у якості ключа доступу. Використання смартфону, паспорту, свідоцтва про реєстрацію транспортного засобу тощо запобігає доступу крадіїв до захищених об'єктів/контрольованих зон, оскільки їм потрібно використовувати телефон, для отримання сигналу, за допомогою якого можна відкрити двері. Також головною перевагою є те, що NFC не може розмагнітитись та його неможливо скопіювати.

При використанні технології NFC використовується дуплексний обмін інформацією, що забезпечує високу швидкість та якість передавання. Пристрій зчитування даних RFID-NFC міток спрацьовує лише на невеликих відстанях, що обмежує можливості зчитування інформації зловмисниками та зменшує витрати енергії під час роботи.

Незважаючи на велику кількість переваг, системи RFID-NFC також мають і недоліки, як от [2, 3]:

– обладнання для такої СКД має велику ступінь енергозалежності: за умови, що мікрочіп не знаходиться в активному стані, він все одно витрачає певний відсоток енергії;

– пристрою для підготовки до роботи потрібен час: на етапі монтажу СКД на основі NFC потрібно правильно розмістити чіп та налаштувати його для правильного та безперебійного функціонування;

– відсутня можливість для швидкого блокування функції. Якщо в якості ключа доступу використовується смартфон з функцією NFC, то у разі його втрати, заблокувати доступ з нього буде важче, оскільки блокування повинно проводитись, коли є фізичний доступ до пристрою.

Методика експериментальних досліджень, означених у роботі, ґрунтується на використанні доступної технології платформи Arduino. Для виконання мети роботи представимо СКД на основі модуля RFID-NFC платформи Arduino. Розглянемо можливості платформи Arduino.

Arduino [10, 11] – це платформа типу «open-sourse», яку засновано на елементарному використанні апаратного та програмного забезпечення. Переважна більшість пристроїв, які виконано на основі платформи Arduino, складаються з базової плати, на якій розміщується мікроконтролер, та модуля розширення, який має назву «shield».

У класичній лінійці пристроїв Arduino в основному використовуються мікроконтролери сімейства Atmel AVR, які розміщуються на різних платах [11]:

- ATmega2560 – плата: Mega;
- ATmega32U4 – плати: Leonardo; Micro; Yun;
- ATmega328 – плати: UnoR3; Mini; NanoR2; Pro; Pro mini;
- ATtiny85 – плати: Digispark;
- ATmega168 – плати: Uno R1; Uno R2; Pro mini; NanoR1.

Для програмування плат Arduino використовується додаток Arduino IDE, який є програмним середовищем розробки і використовує мову програмування C/C++. Абревіатура IDE розшифровується як Integrated Development Environment – інтегроване середовище розробки. Arduino IDE дозволяє писати програму у зручному програмному редакторі, копіювати її та завантажувати машинний код в запам'ятовуючий пристрій плати Arduino.

Середовище Arduino IDE, складається з [10]:

- редактора програмного коду;
- області повідомлень;
- вікна для виводу тексту;
- панелі інструментів.

Програма, яку написано за допомогою середовища Arduino IDE, має назву скетч. Після написання скетчу, перед збереженням, у вікні виведення повідомлень з'являється інформація про наявність існуючих помилок. Також Arduino IDE має вбудовану утиліту Serial Monitor, призначення якої – обмін даними з платформою Arduino. За допомогою утиліти Serial Monitor відбувається налагодження вбудованого програмного забезпечення мікроконтролера, отримання інформації про роботу програми та відправка команд до мікроконтролера через порт USB.

Перед початком розробки системи керування доступом, потрібно розробити алгоритм, за яким буде працювати така система. Алгоритм роботи полягає в наступному:

1. Систему вже встановлено та під'єднано до джерела живлення. Вона знаходиться в активному стані, про що свідчить робота білого світлодіоду. Система очікує на ідентифікатор.

2. У разі сканування ідентифікатора, який не зареєстровано в системі, на дисплей виводиться напис «Wrong card», замок знаходиться в зачиненому стані, доступ до приміщення/приміщень, перед яким встановлено дану СКД, заборонено. Паралельно з цим вмикається червоний світлодіод та звуковий сигнал заборони. У випадку 3-разового прикладання незареєстрованого ідентифікатора, вмикається режим «Тривога». У разі переходу СКД у режим «Тривога» сигнал із системи передається на комп'ютер відділу безпеки та надходить повідомлення у Telegram-Bot.

3. Якщо прикладено зареєстрований ідентифікатор, то на дисплей виводиться напис «Correct card», вмикається зелений світлодіод та звуковий сигнал підтвердження. У цьому випадку замок змінює своє положення на «Відчинено».

4. Після успішної ідентифікації, особа, яка отримала доступ до приміщення/приміщень, відчиняє двері, на які встановлено датчик на основі геркону. Геркон у цій системі керування доступом використовується для контролю зачинення дверей. Після того, як дотягувач зачинив двері, контакти всередині геркону замикаються, а електромеханічний замок переходить у стан «Зачинено». У випадку якщо дотягувач не зачинить двері, через 10 секунд система переходить у стан «Тривоги».

5. Для виходу з приміщення, яке захищається даною СКД, потрібно знову просканувати ідентифікатор та виконати дії, які описано у 4 пункті.

6. У разі переходу системи у стан «Тривога», цей стан буде зберігатися, поки співробітник служби безпеки не вимкне його або за допомогою спеціального сервісного ключа, або дистанційно через робочий комп'ютер, попередньо ввівши логін та пароль, який змінюється щоденно. Система у стані «Тривога» показує причину переходу в цей стан та виводить дані про особу/осіб, які заходили/виходили з приміщення.

Висновки

Експериментальним шляхом досліджено можливості платформи Arduino по створенню СКД на основі RFID технології. Встановлено, що дана платформа має повний арсенал можливостей із розробки будь-

якої гнучкої та надійної СКД. Розроблено алгоритм роботи системи керування доступом підприємства на основі технології RFID/NFC для ідентифікації працівників на певних об'єктах контрольованої зони підприємстві. Доведена доцільність використання технології RFID/NFC, яка найбільш точно відповідає стандартам СКД, де потрібна реєстрація осіб та надання/заборона доступу їм до певних територій/об'єктів. Результати досліджень дали змогу встановити наступне:

- платформа Arduino має всі програмні та апаратні засоби для розробки СКД підприємства на основі технології RFID/NFC завдяки наявності спеціального модуля, який зчитує дані з карт, паспортів тощо;
- середовище розробки Arduino IDE має можливість перевіряти роботу розробленого пристрою;
- доступ у приміщення контрольованої зони надається шляхом прописування у програмний код відповідний ідентифікатор паспорту громадянина України, закордонного паспорту, свідоцтва про реєстрацію транспортного засобу тощо у мікроконтролер Arduino.

Література

1. Царенко В. В. Системи контролю і управління доступом до об'єктів, що охороняються. 2020. https://er.nau.edu.ua/bitstream/NAU/50798/1/%D0%A4%D0%9A%D0%9A%D0%9F%D0%86_2020_123_%D0%A6%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%D0%92.%D0%92..pdf.
2. Системи контролю і управління доступом від А до Я. https://deps.ua/ua/knowegable-base/reference-information/7824.html.
3. Гавриленко І. О. Організація системи керування доступом на приватному підприємстві. 2022. https://ela.kpi.ua/bitstream/123456789/52461/1/HavrylenkoI_mahistr.pdf.
4. Погост О. О. Системи контролю та управління доступом. 2012. https://ukrbukva.net/66525-Sistemy-kontrolya-i-upravleniya-dostupom.html.
5. Об'єкти та процедури, що їх системою контролю і управління доступом. 2008. https://ua-referat.com/Об`єкти_та_процедури_їх_системою_контролю_і_управління_доступом.
6. Критерії оцінки СКУД. Класифікація засобів і систем контролю. Класифікація СКУД. 2014. https://ua-referat.com/Критерії_оцінки_СКУД_Класифікація_СКУД.
7. Системи контролю доступу СКД/СКУД. 2016. https://ukrinfosystems.com.ua/design-and-construction/access-control-systems.
8. Ідентифікація та аутентифікація користувачів. https://sites.google.com/site/identifikaciataautentifikacia/.
9. Що таке NFC і як цю технологію використовувати? https://www.itbox.ua/ua/blog/Scho-take-NFC-i-yak-cyu-tehnologiyu-vikoristovuvati/.
10. What is Arduino? 2023. https://docs.arduino.cc/learn/starting-guide/whats-arduino.
11. Мікроконтроллер Arduino. 2020. https://bitkit.com.ua/shho-take-arduino.

Referenses

1. Tsarenko V. V. Systemy kontroliu i upravlinnia dostupom do obiektiv, shcho okhoroniaiutsia. 2020. https://er.nau.edu.ua/bitstream/NAU/50798/1/%D0%A4%D0%9A%D0%9A%D0%9F%D0%86_2020_123_%D0%A6%D0%B0%D1%80%D0%B5%D0%BD%D0%BA%D0%BE%D0%92.%D0%92..pdf.
2. Systemy kontroliu i upravlinnia dostupom vid A do Ya. https://deps.ua/ua/knowegable-base/reference-information/7824.html.
3. Havrylenko I. O. Orhanizatsiia systemy keruvannia dostupom na pryvatnomu pidpryiemstvi. 2022. https://ela.kpi.ua/bitstream/123456789/52461/1/HavrylenkoI_mahistr.pdf.
4. Pohost O. O. Cystemy kontroliu ta upravlinnia dostupom. 2012. https://ukrbukva.net/66525-Sistemy-kontrolya-i-upravleniya-dostupom.html.
5. Obiekty ta protsedury, shcho yikh systemoiu kontroliu i upravlinnia dostupom. 2008. https://ua-referat.com/Ob`iekty_ta_protsedury_yikh_systemoiu_kontroliu_i_upravlinnia_dostupom.
6. Kryterii otsinky SKUD. Klasyfikatsiia zasobiv i system kontroliu. Klasyfikatsiia SKUD. 2014. https://ua-referat.com/Kryterii_otsinky_SKUD_Klasyfikatsiia_SKUD.
7. Systemy kontroliu dostupu SKD/SKUD. 2016. https://ukrinfosystems.com.ua/design-and-construction/access-control-systems.
8. Identyfikatsiia ta autentyfikatsiia korystuvachiv. https://sites.google.com/site/identifikaciataautentifikacia/.
9. Shcho take NFC i yak tsiu tekhnolohiiu vykorystovuvaty? https://www.itbox.ua/ua/blog/Scho-take-NFC-i-yak-cyu-tehnologiyu-vikoristovuvati/.
10. What is Arduino? 2023. https://docs.arduino.cc/learn/starting-guide/whats-arduino.
11. Mikrokontroller Arduino. 2020. https://bitkit.com.ua/shho-take-arduino.