https://doi.org/10.31891/2219-9365-2023-76-5
УДК 004.056.52

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
МОСТОВИЙ Сергій
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
КОЛІСНИК Вадим
Хмельницький національний університет
e-mail: kolisnykvadim1712@gmail.com

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ RFID-ТЕХНОЛОГІЙ

У статті розглядаються методи та особливості побудови системи контролю та управління доступом до захищених приміщень підприємства з використанням RFID-технологій. Проведено вибір компонентів контролю та управління доступом, сумісних з системами на базі мікроконтролерів Arduino. Наведено приклад практичного використання мікроконтролерів Arduino та RFID-технологій для контролю та управління доступом до захищених приміщень підприємства. Змодельовано систему контролю та управління доступом до режимних об'єктів підприємства. Сформовано узагальнену схему управління системою та розроблено функційну схему контролю та управління доступом.

Ключові слова: система контролю та управління доступом, RFID-технології, структурна схема, функційна схема.

TITOVA Vira, KLOTS Yurii, MOSTOVYI Serhii, KOLISNYK Vadym
Khmelnitskyi National University

ACCESS CONTROL SYSTEM BASED ON RFID TECHNOLOGIES

Implementing security and preventing information leakage in an enterprise is one of the most important and significant problems in many enterprises nowadays. Traditional methods of personal identification, based on the use of passwords or physical media, such as a pass, passport, driver's license, do not always meet modern security requirements and require constant human involvement. One of the most developed and effective means of solving these problems is the use of automatic security alarm systems of various types. The automatic security alarm system is used when equipping various types of premises. At the same time, its purpose is to record any possibility of illegal entry into the protected premises or the protected territory. The basis of the security system is control sensors that transmit information to the central control point. At the same time, the security alarm can be not only autonomous, but also function in a complex with other security systems of the protected object. Automatic security alarm systems allow you to monitor the premises or territory 24 hours a day.

In this work, a system for managing access to the premises at the regime enterprise was developed, which in turn was implemented in the form of a mock-up. The authors conducted a study of the existing access control and management systems and identified the functions that are currently implemented in the ACS. Based on this, a goal was set, as well as requirements for system development were formed, and a conclusion was drawn about the need to develop a system with the lowest economic cost. A structural diagram of the ECU controller and a diagram of the functional structure of the system were developed. The composition of the elements included in the structure of the system is also defined. Modeling was done using selected components and developed structural and functional schemes. Modeling made it possible to verify the correctness of the construction of the system structure and provided the possibility of developing an electrical schematic diagram.

Keywords: access control system, RFID technologies, structural diagram, functional diagram.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Забезпечення безпеки та запобігання витоку інформації на об'єктах інформаційної діяльності є одним з найбільш важливих і критичних питань для багатьох організацій і підприємств на сьогоднішній день. Традиційні методи ідентифікації особистості, засновані на паролях і використанні матеріальних носіїв, таких як перепустки, паспорти і водійські права, не завжди відповідають сучасним вимогам безпеки і завжди вимагають втручання людини [1]. Одним з найбільш розвинених та ефективних засобів вирішення цих проблем є використання різних типів автоматизованих систем контролю та управління доступом (СКУД).

Автоматизовані СКУД використовуються на об'єктах різного типу. Їх призначення – виявлення можливого проникнення на об'єкт або на територію, що охороняються. Основою системи безпеки є датчик контролю, який передає інформацію на центральний пункт управління. При цьому системи безпеки бувають

не тільки автономними, але й можуть працювати в комплексі з іншими системами безпеки на території, що охороняється.

Аналіз досліджень та публікацій

У загальному вигляді СКУД можна представити як сукупність [1]: зчитувальних пристроїв, що здійснюють зчитування ідентифікаційних ознак; керованих перешкоджаючих пристроїв, що забезпечують фізичну перешкоду доступу та керуються за допомогою виконавчих пристроїв (турнікети, двері); виконавчих пристроїв, які забезпечують відкриття або закриття керованих перешкоджаючих пристроїв (електромеханічні, електромагнітні замки, механізми приводу, турнікетів та шлагбаумів); підсистем управління (мікроконтролер), що виконують прийом та обробку інформації з пристроїв зчитування, проведення ідентифікації, надання або заборону доступу шляхом управління виконавчими пристроями, а також передачу інформації системі зберігання даних; системи зберігання даних, яка отримує від мікроконтролера дані та записує в постійний запам'ятовуючий пристрій (ПЗП), також система зберігає базу даних ідентифікаційних ознак.

На сьогоднішній день одними з відомих СКУД можна назвати системи від компанії ASSA ABLOY Global Solutions [2]. В основі архітектури таких систем закладено модульний принцип. Мається на увазі, що система складається з безлічі взаємозамінних приладів, що розподіляються по об'єкту, який захищається,. Усі прилади можуть бути з'єднані у мережу. Як транспортний рівень системи в основному використовуються RS-485-інтерфейс і мережі Ethernet.

До переваг цієї системи можна віднести рішення системою завдань для різних типів приміщень, а саме: реалізація обліку контролю переміщення персоналу на основі аналізу часу приходу/уходу співробітника з підприємства; реалізація безпеки підприємства шляхом інтеграції СКУД із системою пожежної сигналізації – система надає вільний доступ у разі виникнення пожежі.

Ще однією важливою перевагою цих систем є контролер доступу, який можна адаптувати до різних об'єктів компанії. Користувач сам визначає алгоритм роботи. Кожен контролер може обслуговувати двоє дверей і один зчитувач, одні двері і контроль напрямку проходу, турнікети, шлагбауми і шлюзи.

Недоліком системи є вартість обладнання, особливо якщо потрібно організувати контроль доступу на великих територіях. Якщо СКУД інтегрована з системами пожежної безпеки або іншими системами, потрібні додаткові заходи щодо захисту території (наприклад, відеоспостереження) для запобігання несанкціонованому доступу, відповідно витрати компанії збільшуються.

Ще одною відомою на ринку СКУД є компанія ZKTeco, яка пропонує як невеликі автономні системи, так і інтегровані рішення, які можуть об'єднувати різні системи. Виробники компанії пропонують системи з різними вимогами до безпеки [3].

Перевагами систем ZKTeco є широкий спектр вирішуваних завдань, детальні та зрозумілі інструкції з встановлення та використання систем, безкоштовне програмне забезпечення, виробництво біометричних інструментів та широкий асортимент продукції. Система інтегрована з іншими виробничими підсистемами, що забезпечує масштабованість. Недоліком системи є висока вартість комплексу та окремого обладнання.

Аналіз існуючих аналогічних систем показує, що ці системи мають спільний недолік – високу вартість апаратного та програмного забезпечення. Тому потрібно підібрати елементи, необхідні для побудови системи, яка буде найменш дорогою, але не поступатиметься за функціональністю іншим існуючим системам.

Формулювання цілей статті

Метою роботи є: розробка мікроконтролерної системи керування доступом до приміщень на режимному підприємстві з найменшою економічною вартістю.

Виклад основного матеріалу

Система контролю та управління доступом, що розробляється, повинна забезпечувати: вмикання/вимикання живлення системи; запис ідентифікаційних ключів в пам'ять системи та їх зберігання; подачу сигналу на відкривання керованого запобіжного пристрою при зчитуванні зареєстрованого в пам'яті системи ідентифікаційного ключа; подання сигналу на заборону відкривання керованого запобіжного пристрою при зчитуванні незареєстрованого в пам'яті системи ідентифікаційного ключа; повідомлення звуковим та світловим сигналом про отримання чи заборону доступу; автоматичне формування сигналу закриття на виконавчі пристрої за відсутності факту проходу; надання різних рівнів доступу; збереження ідентифікаційних ознак у пам'яті системи при обриві зв'язку із системою зберігання даних; фіксацію спроби несанкціонованого доступу у системі зберігання даних; передачу даних про надання доступу або його заборону в систему зберігання даних (до бази даних (БД)) та їх подальше зберігання; використання інтерфейсу RJ-45 та мережі Ethernet, як транспортного рівня системи.

Рівні доступу розділені відповідно до посади працівника. Менеджери та директори компанії мають необмежений доступ до приміщень та систем зберігання даних. Працівники поділяються на дві категорії

прав: з високими та низькими привілеями. Працівники з низьким рівнем привілеїв мають доступ до зон вільного доступу компанії. Працівники з високим рівнем привілеїв мають доступ до деяких зон з обмеженим доступом на додаток до вищезазначених прав, але не мають доступу до систем зберігання даних. Відповідно до поставлених завдань та вимог, була розроблена структурна схема системи, як показано на рис. 1.

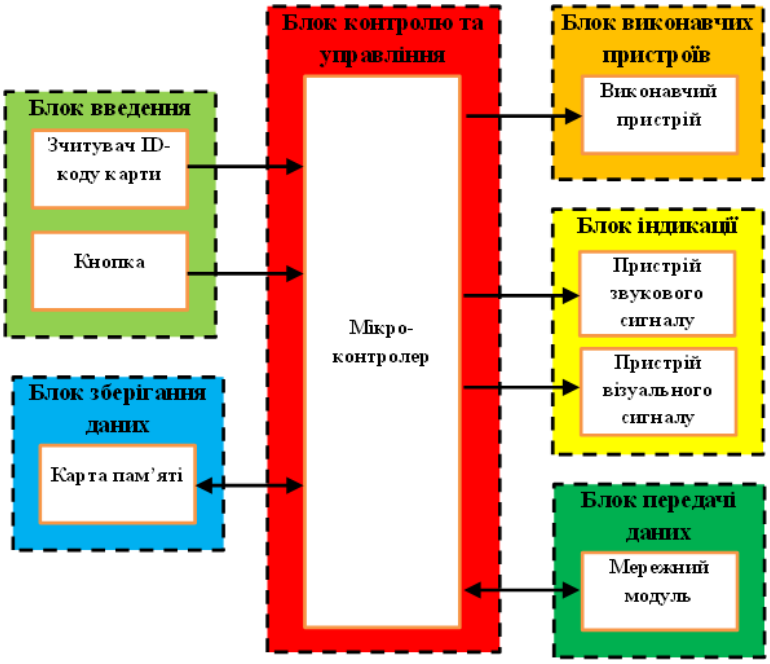

Рис. 1. Структурна схема системи контролю та управління доступом

Блок контролю та управління є "ядром" всієї системи і являє собою мікроконтролер (МК). МК отримує ідентифікаційні ключі або коди (ID-коди) від зчитувача. Потім він отримує доступ до системної карти пам'яті за умови отримання даних від зчитувача. Далі він приймає рішення на основі отриманих сигналів та даних і надсилає відповідні сигнали на виконавчий блок та блок індикації, а також надсилає необхідні дані на блок передачі даних.

Якщо МК знаходить необхідний ідентифікаційний код на карті пам'яті, тобто якщо відповідь позитивна, МК надсилає сигнал на виконавчий блок, який певним чином активує звуковий та візуальний сигнальний пристрій у блоці індикації (лунає сигнал певного тону та тривалості, а також загоряється зелений індикатор). Потім МК надсилає ці дані до мережного модуля, звідки вони передаються в мережне середовище компанії.

Якщо МК не отримує позитивної відповіді, привід залишається в початковому стані, а блок індикації надсилає сигнал акустичному та візуальному обладнанню (лунає сигнал, що відрізняється за тональністю та тривалістю від попередньої версії, і загоряється червоний індикатор). Нарешті, МК надсилає на мережний модуль інформацію про спробу входу в зону за допомогою картки, ідентифікаційний код якої відсутній на карті пам'яті системи.

Кнопки використовуються для управління пристроями перешкод при необхідності виходу з приміщення і розміщуються біля дверей приміщення. Коли МК отримує сигнал від кнопки, МК сприймає його як вищезгадану позитивну відповідь.

Розроблена структурна схема дозволила визначити основні функційні модулі мікроконтролерної системи розроблюваної СКУД, реалізувати її функційні процеси та вибрати елементи, необхідні для складання системи.

На основі досліджень існуючих систем контролю та управління доступом [4-6], а також відповідно до вищезазначених вимог та розробленої структурної схеми визначено конфігурацію компонентів, необхідних для розроблюваної системи. Найбільш важливим та основоположним елементом є МК. В системі використовується мікроконтролер AVR Atmega328 фірми Atmel.

Як пристрій зчитування обраний RFID-зчитувач RC522 (рис. 2.а). Зі зчитувачами визначаються і мітки/ключі (магнітні карти). До виконавчих пристроїв належать електромагнітні замки, електромагнітні засувки та механізми приводу воріт або поворотної платформи, залежно від місця розташування системи на підприємстві. У даній СКУД електромагнітні замки обрані так, що система встановлюється для контролю доступу в приміщення через двері (рис 2.б.). В системі також необхідні елементи індикації для відображення статусу про надання доступу або його відмови. До таких відносяться світлодіоди та

звуковипромінювачі (зумери) (рис. 2.в). Для зберігання бази ІД-кодів використовується зовнішня пам'ять, а саме картка microSD з адаптером. Для взаємодії контролера з microSD карткою визначено модуль SD Card.

а) б) в)

Рис. 2. Складові елементи СКУД: а – зчитувач RFID-RC522, б – електромагнітний замок, в – модуль електромеханічного реле зі світлодіодами

Відповідно до розробленої структурної схеми та певного складу компонентів, розроблено функційну схему системи (рис. 3).

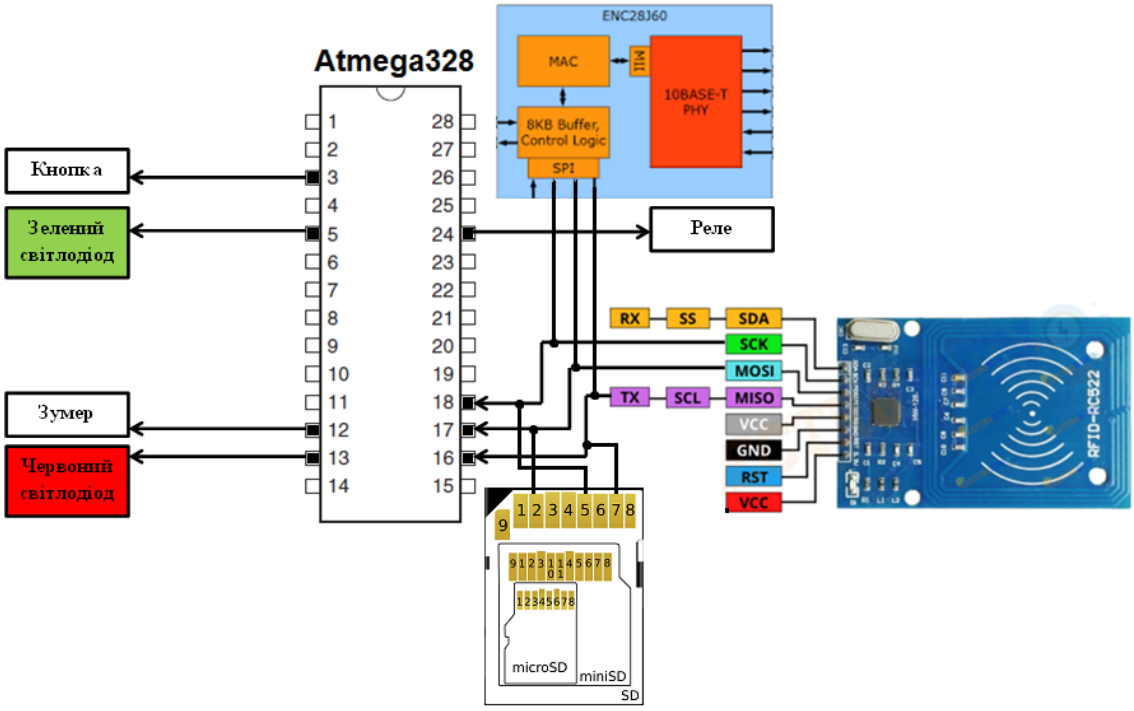

Рис. 3. Функційна схема системи контролю та управління доступом

Розроблена функційна схема дозволяє визначити алгоритми роботи системи, створити модель працюючої системи та спроєктувати схеми блоків контролю та управління доступом.

Для моделювання системи на основі розробленої функційної схеми було створено натурну модель. На макетній платі було встановлено "ядро" системи - платформу Arduino Nano на базі AVR Atmega328 [7]. Далі за допомогою з'єднувальних проводів були підключені RFID-зчитувач, модуль SD-карти, Ethernet-модуль, світлодіоди, зумер і відповідні резистори, кнопки і сервоприводи, що використовуються в якості пристроїв безпеки. Після підключення живлення робота СКУД починається з процесу ініціалізації, під час якого активується програма, що зберігається в МК. Процес активного стану контролює стан зчитувача та кнопок. Коли картка підноситься до зчитувача, система реагує і, в залежності від того, чи є код картки в базі даних, МК вмикає відповідний світлодіод, зумер і реле (якщо доступ до картки дозволено). Сигнали світлодіода та зумера надалі називаються сигналами доступу. Коли сигнал зчитується з кнопки, сигнал також надсилається на зелений світлодіод, зумер та реле.

Алгоритм ідентифікації ID-коду картки, керування перешкоджаючим пристроєм, і відправлення даних на сервер по мережі:

Крок 1. Увімкнення живлення, запуск ініціалізації мікроконтролерної системи.

Крок 2. Очікування сигналів із блоку введення (зчитувач та кнопка).

Крок 3. Перевірка на наявність карти в області зчитувача. Якщо картка відсутня в області зчитувача, виконується крок 2. Інакше крок 4.

Крок 4. Зчитування коду картки.

Крок 5. Перевірка коду картки на відповідність до кодів у пам'яті системи. Якщо код знайдено, крок 6, інакше сигнали про заборону доступу (сигнал червоного світлодіода, звуковий сигнал) і перехід до кроку 8.

Крок 6. Сигнали про надання допуску (сигнал зеленого світлодіода та звуковий сигнал).

Крок 7. Відкриття запобіжного пристрою, затримка 5 секунд, закриття запобіжного пристрою.

Крок 8. Передача даних про подію на сервер по локальній мережі. На сервер передається ID-код прочитаної карти та статус.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

В ході дослідження було розроблено та впроваджено систему на основі RFID-технології для контролю та управління доступом до приміщення на режимному підприємстві, яка у свою чергу була реалізована у вигляді макета.

Авторами було проведено огляд існуючих систем контролю та управління доступом та визначено функції, які наразі реалізовані в СКУД. На цій основі були поставлені цілі, сформовані вимоги до розробки системи та зроблені висновки про необхідність розробки системи з найменшими економічними витратами. Створено структурну схему контролера СКУД та функційну структуру системи. Також було визначено склад елементів в структурі системи. Проведено моделювання з використанням обраних компонентів та розроблених структурної та функційної схем. Моделювання дозволило перевірити правильність обраної структури системи та є основою для подальшої розробки принципової схеми системи та її апаратної реалізації.

Розроблена система відповідає всім вимогам і має ряд переваг, серед яких низька вартість, компактність і простота використання в порівнянні з аналогічними продуктами. Система може бути використана як у загальному приватному секторі, так і в інформаційних установах з захищеними приміщеннями.

Література

1. Системи доступу: підручник/ Г. Г. Бортник, В. М. Кичак, О. В. Стальченко. Вінниця: ВНТУ, 2010. 298 с.

2. Системи контролю доступу ASSA ABLOY Global Solutions: [Електронний ресурс] – Режим доступу: https://www.assaabloyglobalsolutions.com/en/products

3. Системи контролю доступу ZKTeco: [Електронний ресурс] – Режим доступу: https://zktecoua.com/ua/solutions/skud/

4. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури/ Ю. Васильєв// ДержНДІ Спецзв‘язку. 2015. С. 58-60.

5. Характеристика та загальні вимоги до системи контролю і управління доступом/ М.О. Омельченко// Сучасний захист інформації. 2020. №4 (44). С.46-50.

6. Аналіз та класифікація систем контролю та управління доступом на підприємстві/ О.К. Юдін, О.М. Весельська// Наукоємні технології. 2018. № 2 (38). С. 220-225.

7. Основи мікропроцесорної техніки/ В. С. Баран, Г. Г. Власюк, Ю. О. Оникієнко, О. І. Смоленська. КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2019. 140 с.

References

1. Systemy dostupu: pidruchnyk/ H. H. Bortnyk, V. M. Kychak, O. V. Stalchenko. Vinnytsia: VNTU, 2010. 298 s.

2. Systemy kontroliu dostupu vid kompanii ASSA ABLOY Global Solutions: [Elektronnyi resurs] – Rezhym dostupu: https://www.assaabloyglobalsolutions.com/en/products

3. Systemy kontroliu dostupu ZKTeco: [Elektronnyi resurs] – Rezhym dostupu: https://zktecoua.com/ua/solutions/skud/

4. Klasyfikatsiia ta analiz zahroz informatsiinii bezpetsi v kliuchovykh systemakh informatsiinoi infrastruktury / Yu. Vasyliev// DerzhNDI Spetszv‘iazku. 2015. S. 58-60.

5. Kharakterystyka ta zahalni vymohy do systemy kontroliu i upravlinnia dostupom/ M.O. Omelchenko// Suchasnyi zakhyst informatsii. 2020. №4 (44). S.46-50.

6. Analiz ta klasyfikatsiia system kontroliu ta upravlinnia dostupom na pidpryiemstvi/ O.K. Yudin, O.M. Veselska// Naukoiemni tekhnolohii. 2018. № 2 (38). S. 220-225.

7. Osnovy mikroprotsesornoi tekhniky/ V. S. Baran, H. H. Vlasiuk, Yu. O. Onykiienko, O. I. Smolenska. KPI im. Ihoria Sikorskoho. Kyiv: KPI im. Ihoria Sikorskoho, 2019. 140 s.