

Для цитирования: Бужинская Н.В., Васева Е.С., Искандаров Р.Н., Шубина Н.В. Система контроля и управления доступом на базе микроконтроллеров ARDUINO. Вестник Дагестанского государственного технического университета. Технические науки. 2019;46(1): 103-112. DOI:10.21822/2073-6185-2019-46-1-103-112

For citation: Buzhinskaya N. V., Vaseva E. S., Iskandarov R. N., Shubina N. V. System of control and management of access on the basis of ARDUINO microcontrollers. Herald of Daghestan State Technical University. Technical Sciences. 2019; 46 (1): 103-112. (In Russ.) DOI:10.21822/2073-6185-2019-46-1-103-112

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.78:681.139.32

DOI:10.21822/2073-6185-2019-46-1-103-112

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ МИКРОКОНТРОЛЛЕРОВ ARDUINO

Бужинская Н.В.², Васева Е.С.³, Искандаров Р.Н.⁴, Шубина Н.В.¹

¹⁻³ Нижнетагильский государственный социально-педагогический институт (филиал)

¹⁻³ Российского государственного профессионально-педагогического университета,

¹⁻³ 622031, Свердловская обл., г. Нижний Тагил, ул. Красногвардейская, 57, Россия,

⁴ ООО «Баранчинский электромеханический завод имени Калинина»,

⁴ 624315, Свердловская обл., г. Кушва, п. Баранчинский, ул. Ленина, 2, Россия,

¹ e-mail:nata-shubina@yandex.ru, ² e-mail:nadezhda_v_a@mail.ru,

³ e-mail:e-s-vaseva@mail.ru, ⁴ e-mail:grim_sleeper@mail.ru

Резюме. Цель. Целью исследования является выбор методов и средств для эффективной модернизации системы безопасности, существующей на предприятии. **Метод.** Усовершенствование пропускного режима предлагается осуществить с помощью системы контроля и управления доступом на базе микроконтроллеров ARDUINO. Для выделения функций данной системы и требований к ней были построены UML-диаграммы. На основе этих диаграмм была разработана принципиальная электрическая схема аппаратной части системы с указанием всех входящих в нее элементов. На следующем этапе был предложен алгоритм работы аппаратной части системы контроля и управления доступом. Реализация части алгоритма для обмена информацией между устройством и информационной системой продемонстрирована в виде скетча на примере передачи пакетов по сети Ethernet по протоколу TCP. Для взаимодействия между системой и конечным пользователем был разработан интуитивно-понятный интерфейс. Необходимая информация хранится в базе данных, созданной в среде Microsoft SQL Server. **Результат.** Разрабатываемая система была протестирована на предприятии посредством скетчей и мультиметра. Результаты тестирования позволяют сделать вывод, что система готова к внедрению. **Вывод.** В статье рассмотрен один из методов модернизации существующей системы контроля и управления доступом за счет более удобного интерфейса и добавления функций входа/выхода.

Работа выполнена по заказу предприятия ООО «Баранчинский электромеханический завод им. Калинина».

Ключевые слова: автоматизированная система контроля и управления доступом, проектирование, микроконтроллер, ARDUINO, скетч, интерфейс

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

SYSTEM OF CONTROL AND MANAGEMENT OF ACCESS ON THE BASIS OF ARDUINO MICROCONTROLLERS

Nadezhda V. Buzhinskaya², Elena S. Vaseva³, Rustam N. Iskandarov⁴, Natalya V. Shubina¹

¹⁻³Nizhny Tagil State Social-Pedagogical Institute (branch),

¹⁻³Russian State Vocational-Pedagogical University»,

¹⁻³57, Krasnogvardeyskaya Str., Sverdlovsk Region, Nizhny Tagil 622031, Russia,

⁴LLC «Kalinin Baranchinsky Electromechanical Plant»

⁴2, Lenin Str., Sverdlovsk region, Kushva, p. Baranchinsky 624315, Russia,

¹e-mail:nata-shubina@yandex.ru, ²e-mail:nadezhda_v_a@mail.ru,

³e-mail:e-s-vaseva@mail.ru, ⁴e-mail:grim_sleeper@mail.ru

Abstract. Objectives The aim of the study is to select methods and means for the effective modernization of the security system existing in the enterprise. **Method** It is proposed to improve the access control mode using the access control system based on ARDUINO microcontrollers. To highlight the functions of the system and the requirements for it were built UML-diagrams. On the basis of these diagrams, the balls have developed a schematic electrical diagram of the hardware of the system with an indication of all its elements. At the next stage, an algorithm was proposed for the operation of the hardware of the access control system. The implementation of a part of the algorithm for information exchange between the device and the information system is shown in the form of a sketch using the example of packet transmission over an Ethernet network using the TCP protocol. An intuitive interface has been developed for interaction between the access control system and the end user. The necessary information is stored in a database created in a Microsoft SQL Server environment. **Result** The developed system was tested at the enterprise by means of sketches and a multimeter. Test results allow us to conclude that the system is ready for implementation. **Conclusion** The article describes one of the methods for upgrading the existing access control system through a more user-friendly interface and the addition of entry/exit functions.

Acknowledgments The work was commissioned by the company LLC «Kalinin Baranchinsky Electromechanical Plant».

Keywords: automated access control system, design, microcontroller, ARDUINO, sketch, interface

Введение. В настоящее время автоматизированные системы контроля и управления доступом (СКУД) являются составной частью информационной инфраструктуры и незаменимым элементом системы безопасности современного предприятия [1-4].

В общем случае под системой контроля и управления доступом понимают совокупность программно-технических и организационно-методических средств, с помощью которых решается задача контроля и управления помещениями предприятия, а также оперативный контроль за передвижением персонала и временем его нахождения на территории предприятия [5]. С помощью системы контроля и управления доступом, предприятие имеет возможность поднять уровень общей безопасности, а также сократить затраты на ее обеспечение [6]. Кроме того, СКУД предполагает меньшее количество персонала для обслуживания, она экономична в потреблении электроэнергии [7].

Для того, чтобы система четко и бесперебойно выполняла свои функции, решала все поставленные задачи и обеспечивала максимальный экономический эффект от своей эксплуатации, она должна быть грамотно спроектирована, качественно смонтирована, интегрирована с другими системами безопасности [8-9]. Проектирование и разработку СКУД будем рассматривать для предприятия ООО «Баранчинский электромеханический завод им. Калинина».

Постановка задачи. Анализ деятельности предприятия ООО «Баранчинский

электромеханический завод им. Калинина» выявил проблемы в работе пропускной системы. Они обусловлены тем, что имеющаяся на предприятии СКУД имеет ряд недостатков:

- низкая отказоустойчивость;
- неудобный для администрирования системы интерфейс;
- отсутствие возможности масштабирования;
- дорогостоящие комплектующие;
- отсутствие функции ограничения входа/выхода в неположенное время.

Для решения указанных проблем возникла необходимость в усовершенствовании данной системы.

Методы исследования. На центральной и малой проходной завода установлены контроллеры PERCo-CT/L04, турникеты – триподы PERCo-TTR-04, считыватели PERCo-IR03.

Проход осуществляется по бесконтактным проксимити-картам Mifare. Эти карты позволяют не только осуществлять доступ, но и хранить в памяти записанную на них информацию [10].

Вся система функционирует на программном обеспечении «Барс.СКД».

Разрабатываемая СКУД будет служить дополнением к существующей охранной системе предприятия. Она будет нацелена на усовершенствование пропускного режима складских помещений на предприятии.

Проектирование СКУД. Первый этап работы предполагает выделение требований к системе и определение ее функционала. Для решения данной задачи были построены UML-диаграммы, предназначенные для графического описания особенностей работы программных продуктов [11, 12].

На диаграмме вариантов использования (use case diagram) показаны отношения между актерами и вариантами использования (рис. 1).

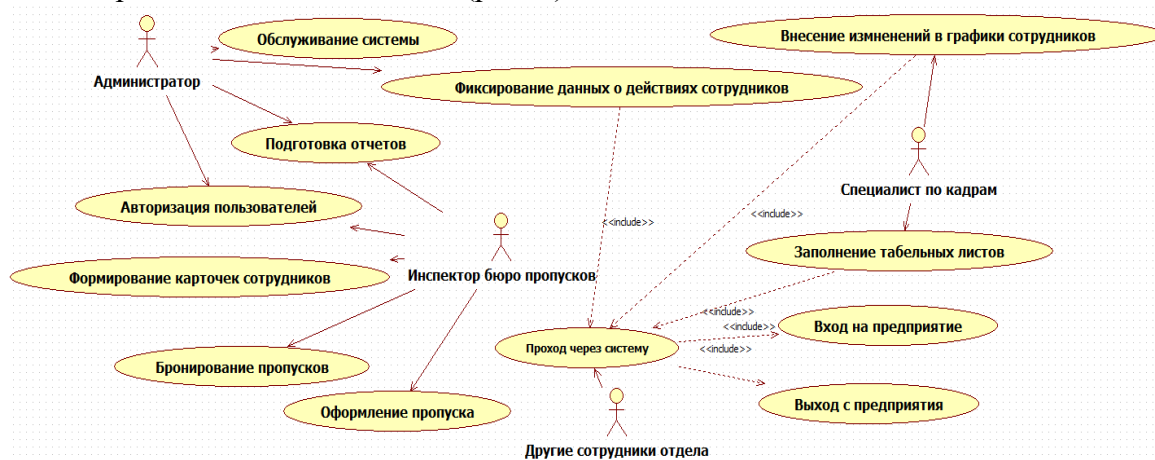


Рис. 1. Диаграмма вариантов использования, иллюстрирующая требования к системе
Fig. 1. Chart of use cases illustrating system requirements

На рис. 1 отражены администратор системы, инспектор бюро пропусков, специалист по кадровому учету и другие сотрудники. Инспектор бюро пропусков формирует карточки сотрудников, привязывает к ним идентификатор метки (RFID) и передает данные в систему контроля доступом. Администратор системы следит за работоспособностью системы, создает и управляет учетными записями пользователей. Специалист по кадрам вносит изменения в структуру подразделений, которая используется СКУД для разграничения доступа по определенным зонам контроля, создает отчеты на основании статистики. Статистика формируется автоматически на основании информации переданной микроконтроллером в программную часть программно-аппаратного комплекса (ПАК). Система взаимодействует с остальными сотрудниками, считывая их пропуска (метки) и запрещая/разрешая проход через определенную зону контроля, а также фиксирует их проход в журнале событий.

Рассмотреть более детально алгоритм работы аппаратной части СКУД позволяет диаграмма состояний (рис. 2).

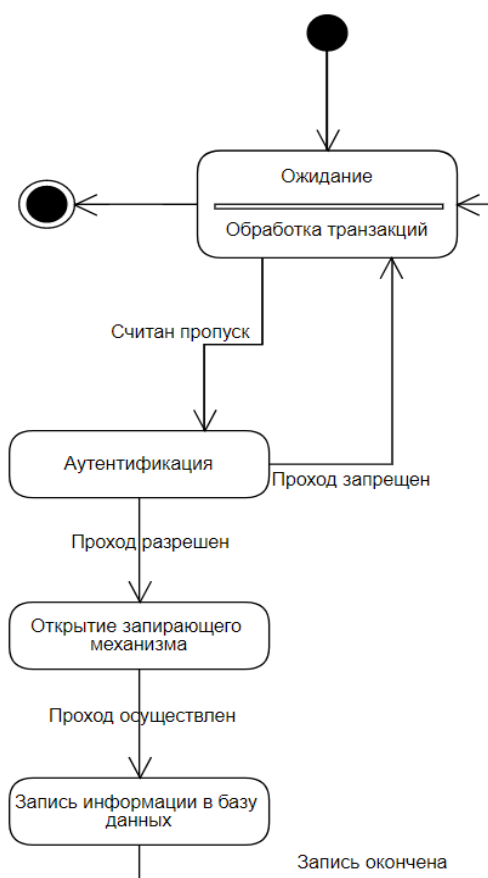


Рис. 2. Диаграмма состояний, на которой продемонстрирован алгоритм работы аппаратной части
Fig. 2. The activity diagram, which demonstrates the algorithm of the hardware

При прикладывании пропуска сотрудником и считывании данных происходит аутентификация. В результате аутентификации система реагирует на событие: открывает запирающий механизм или игнорирует действия сотрудника, переходя в изначальное состояние. При выполнении вышеуказанных действий система записывает все события в журнал.

Разработка аппаратной части. В качестве платформы для разработки контроллера СКУД используется платформа Arduino Mega 2560 R3 [13-16]. По способу управления разрабатываемый контроллер относится к сетевым, что позволяет создать СКУД любой степени сложности. К платформе Arduino добавлена плата расширения Ethernetshield W5100 forMega. Данная плата позволяет использовать передачу данных по сети Ethernet, а также имеет разъем для подключения SD-карты, используемой для хранения информации. Для считывания карт к контроллеру подключен считыватель RC-522, который позволяет считывать данные с проксимити-карт.

В качестве исполнительных устройств, для осуществления пропускного режима в системе контроля ограниченного доступа используются электромагнитные замки.

В итоге аппаратная часть проектируемого ПАК будет состоять из следующих элементов:

- плата Arduino Mega 2560 R3 – 1 шт;
- плата расширения Ethernet W5100 – 1 шт;
- считыватель меток RFID RC522 – 3 шт;
- управляемое реле keyes_srly – 1 шт;
- светодиод красный/зеленый – 2 шт;
- резистор 220 Ом – 2 шт;
- печатная плата 9x15 – 1 шт;
- плата Arduino Nano – 2 шт;

- оптический кросс 8 портов FC/ST – 1 шт;
- коммуникационный модуль RS-485 – 5 шт;
- модуль часов реального времени – 1 шт;
- спикер Zimmershield – 1 шт.

На рис. 3 представлена принципиальная электрическая схема, отображающая взаимосвязь элементов в проектируемой системе. В ГОСТ 2.701-2008 принципиальная схема определяется как «схема, определяющая полный состав элементов и связей между ними и, как правило, дающая детальное представление о принципах работы изделия» [17].

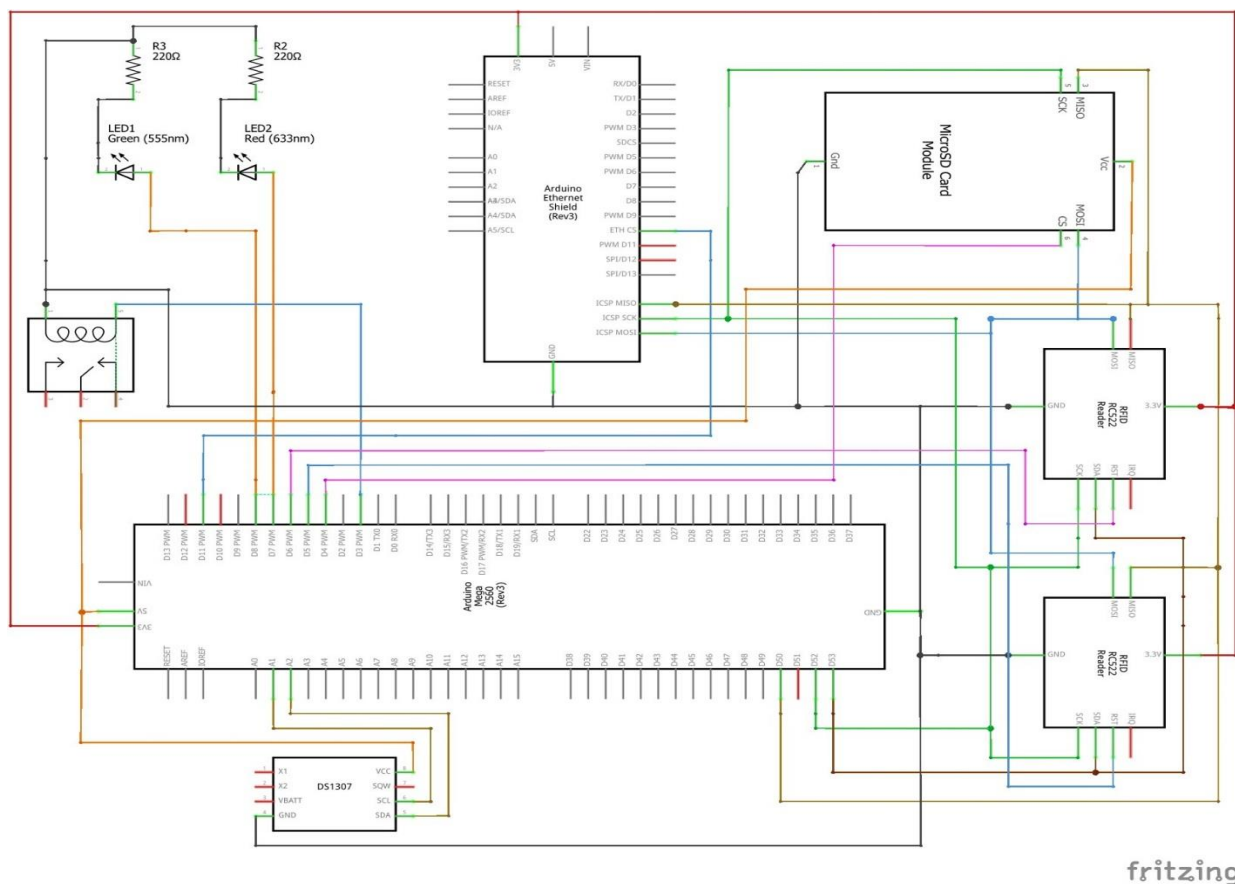


Рис. 3. Принципиальная электрическая схема
Fig. 3. Schematic circuit

Сборка контроллера начинается с подготовки печатной платы. Для соединения элементов устройства на плату наносятся контактные дорожки. После нанесения дорожек на плате располагаются элементы устройства и их выводы запаиваются к контактным площадкам. Результат проделанной работы представлен на рис. 4. В дальнейшем устройство размещается в корпусе.

С метки считывается идентификатор и переводится в десятичную систему счисления. Полученное число сравнивается с имеющимися на flash-карте сигнатурами. Если проверка успешна, то спикер контроллера воспроизводит одиночный сигнал, и, одновременно на карте памяти сохраняется соответствующий лог файл.

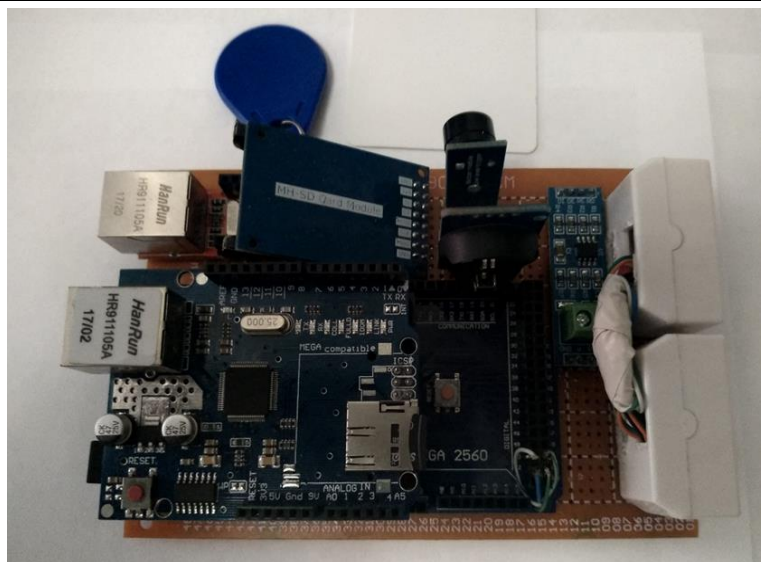


Рис. 4. Расположение элементов СКУД на печатной плате
Fig. 4. The location of the access control elements on the PCB

Исполняющее устройство в свою очередь переводится в состояние отличное от текущего на указанный промежуток времени. В противном случае, спикер контроллера воспроизводит два последовательных звуковых сигнала и исполняющее устройство не меняет свое состояние.

Разработка программной части. Программная часть состоит из двух скетчей, для написания которых была использована среда разработки ArduinoIDE [18]. Обмен информацией между устройством и информационной системой осуществляется путем передачи пакетов по сети Ethernet по протоколу TCP.

Разработка пользовательского интерфейса. Пользовательский интерфейс (рис. 5) выступает в качестве звена взаимодействия между СКУД и конечным пользователем. Он представляет собой окно, на котором расположены различные элементы взаимодействия: кнопки, таблицы, изображения, графический указатель, элементы прокрутки [19].

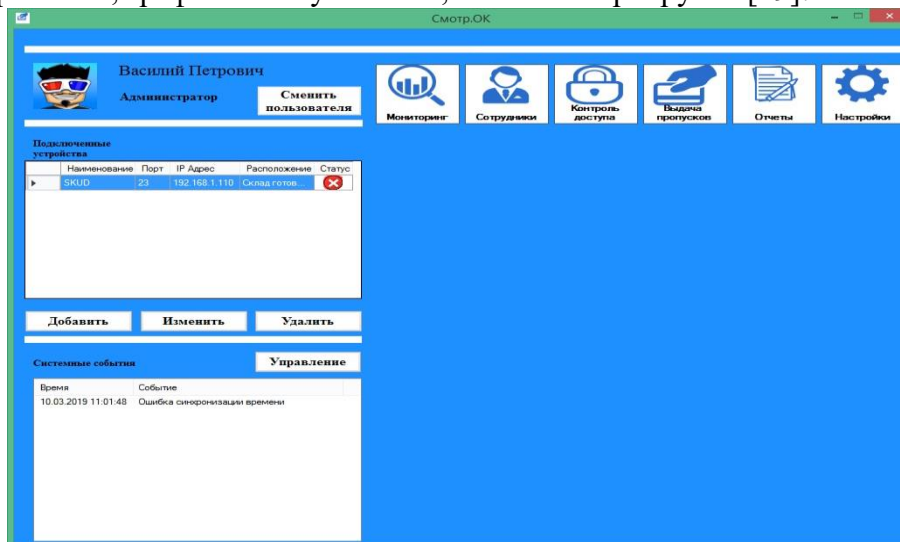


Рис. 5. Пользовательский интерфейс системы
Fig. 5. System user interface

Пользователю, при наличии прав, доступны следующие функции: авторизация, управление пользователями системы, просмотр системных журналов, настройки подключения сетевых аппаратных устройств, работа с отчетами, формирование карточек сотрудников, работа с пропусками, работа с производственным календарем, работа с табельными листами, редактирование внесенной структуры предприятия.

Каждый сотрудник имеет право доступа в определенные зоны в установленное время. Информация о «разрешениях доступа» хранится в базе данных, реализованной посредством СУБД Microsoft SQL Server [20]. В дальнейшем информационная система генерирует SQL запросы для получения/изменения данных.

Обсуждение результатов. Для тестирования работоспособности устройства применяются специально подготовленные тестовые скетчи (листинг 1) и мультиметр.

Все основные элементы устройства тестируется по отдельности. В частности отдельно тестируется работа Ethernet-модуля, модуля RS485, модуля часов реального времени, а также связующие элементы (дорожки печатной платы, разъемы).

Листинг 1. Фрагмент тестового скетча для проверки RFID
Listing 1. RFID test fragment

```
void RFID()
{
  if (rfid.isCard())
  {
    if (rfid.readCardSerial())
    {
      if (rfid.serNum[0] != serNum0
        &&rfid.serNum[1] != serNum1
        &&rfid.serNum[2] != serNum2
        &&rfid.serNum[3] != serNum3
        &&rfid.serNum[4] != serNum4)
      {
        serNum0 = rfid.serNum[0];
        serNum1 = rfid.serNum[1];
        serNum2 = rfid.serNum[2];
        serNum3 = rfid.serNum[3];
        serNum4 = rfid.serNum[4];
        serNumTotal = String(serNum0)+String(serNum1)+String(serNum2)+String(serNum3)+String(serNum4);
        for (byte i = 0; serNumTotal.length() < 15; i++) // Метка дописывается до 15 символов
        {serNumTotal = serNumTotal + 1;}
        digitalWrite(SerialTxControl, RS485Transmit);
        Serial.print(serNumTotal);
        delay(20);
        digitalWrite(SerialTxControl, RS485Receive);
      }
    }
    else
    { rfidres ++;
      if (rfidres == 70) {
        serNum0 = 0;
        serNum1 = 0;
        serNum2 = 0;
        serNum3 = 0;
        serNum4 = 0;
        rfidres = 0;
      } } }
    rfid.halt();
  }
}
```

Поскольку известен функционал программы, основным методом тестирования является метод «Черного ящика» [21, 22]. В процессе тестирования исследовалась работа каждой функции на всей области определения. При этом основное внимание акцентируется на работе основных аспектов системы.

С помощью данных тестов отслеживались результаты:

- выполнения функций программы [23];
- приема исходных данных;
- обработки данных [24];
- сохранения целостности внешней информации [25].

Результаты тестирования представлены в табл. 1.

Таблица 1. Фрагмент таблицы результатов тестирования работы системы
Table 1. Fragment of the system test results table

| № | Описание Description | Входные данные Input data | Ожидаемый результат Expected Result |
|---|---|--|---|
| 1 | Проверка цепей на наличие обрыва Check for open circuit | Проверка проводилась при помощи мультиметра в режиме прозвонки The test was carried out using a multimeter in dialing mode | Обрыв в цепи не обнаружен Open circuit not detected |
| 2 | Проверка цепей на наличие короткого замыкания Checking for short circuits | Проверка проводилась при помощи мультиметра в режиме прозвонки The test was carried out using a multimeter in dialing mode | Короткого замыкания не найдено Short circuit not found |
| 3 | Проверка считывателей, платы расширения Ethernet, модуля часов реального времени, прочие платы расширения Verification of readers, Ethernet expansion cards, real-time clock module, other expansion cards | Проверка производилась при помощи тестовых скетчей, в результате все платы расширения подключены правильно и функционируют исправно The test was performed using test sketches, as a result, all expansion cards are connected correctly and function properly. | Платы расширения протестированы по отдельности и исправны Expansion cards are tested separately and in good condition. |
| 4 | Попытка ввода несуществующих данных пользователя Attempt to enter non-existing user data | Несуществующий логин и/или пароль Nonexistent login and / or password | Авторизация не удалась Login failed |
| 5 | Попытка просмотра списка пользователей Attempt to view user list | Щелчок мыши по вкладке «Пользователи» Click on the tab "Users" | Открылась форма «Пользователи» The form "Users" has opened |
| 6 | Попытка просмотра списка сотрудников Attempt to view the list of employees | Щелчок мыши по вкладке «Сотрудники» Click on the tab "Employees" | Открылась форма «Сотрудники» The form "Employees" has opened |

В результате проведенных тестов установлено, что все компоненты аппаратной и программной части СКУД исправны и функционируют согласно требованиям.

Вывод. Разработанная система ориентирована не только на текущее состояние складского объекта, но и на перспективу. Она позволит наращивать возможности функционирования, благодаря гибкой структуре и возможности изменения кода. В дальнейшем планируется увеличивать масштабы системы и дополнить ее новыми компонентами, такими как охранно-пожарная сигнализация, видеонаблюдение, платежная система, инженерные системы здания, информационные системы и системы коммуникаций организации.

Библиографический список

1. Барсуков В. С. Безопасность: технологии, средства, услуги. – М. : КУДИЦ – ОБРАЗ, 2001. – 496 с.
2. Гафнер В. В. Информационная безопасность: Учебное пособие.– Ростов на Дону. : Феникс, 2010. – 324 с.
3. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие. – Ст. Оскол : ТНТ, 2010. – 384 с.
4. Охрана труда и промышленная охрана. [Электронный ресурс]. URL: <http://prom-nadzor.ru> (дата обращения 25.05.2019).
5. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2012. – 16 с.
6. Бадиков А. В., Бондарев П. В. Системы контроля и управления доступом. Лабораторный практикум. – М. : НИЯУ МИФИ, 2010. – 128 с.

7. Волхонский В. В. Некоторые вопросы разработки методологии построения систем контроля доступа и выбора технологии идентификации // Информационно-управляющие системы. – 2012. – № 4. – с. 78–83.
8. Волхонский В. В. Системы контроля и управления доступом. – СПб. : Университет ИТМО, 2015. – 200 с.
9. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М. : Горячая линия-Телеком, 2010. – 272 с.
10. Считыватель бесконтактный PERCo-IR03. Руководство по эксплуатации. [Электронный ресурс]. URL: http://www.etk-elcom.ru/docs/PERCo_IR03D_Rukovodstvo_po_ekspluatatsii.pdf (дата обращения 25.05.2019).
11. Каюмова А. В. Визуальное моделирование систем в StarUML: учебное пособие. – Казань. Казанский федеральный университет, 2013. – 104 с.
12. Daoust N. UML Requirements Modeling For Business Analysts: Steps to Modeling Success. Technics Publications, 2012. – 268 p.
13. Интернет-сайт Arduino.ru. [Электронный ресурс]. URL: <http://arduino.ru> (дата обращения 25.05.2019).
14. Arduino. [Электронный ресурс]. URL: <https://www.arduino.cc/> (дата обращения 25.01.2019).
15. Margolis M. Arduino Cookbook. O'Reilly Media, Inc., 2011. – 662 p.
16. Сомер Ул. Программирование микроконтроллерных плат Arduino/Freduino. – СПб. : БХВ-Петербург, 2017. – 240 с.
17. ГОСТ 2.701-2008. Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению. – М. : Стандартинформ. 2009. – 16 с.
18. Петин В. А. Проекты с использованием контроллера Arduino. – СПб. : БХВ-Петербург, 2019. – 496 с.
19. Бирман И. Пользовательский интерфейс. – М. : Дизайн-бюро Артёма Горбунова, 2017. – 363 с.
20. Кузнецов С. Д. Основы баз данных. – М. : Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2007. – 484 с.
21. Куликов С. Тестирование программного обеспечения. Базовый курс. – Минск : Четыре четверти, 2017. – 312 с.
22. Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем. – СПб. : Издательский Дом Питер, 2004. – 321 с.
23. Beizner V. Software Testing Techniques. – Itp – Media, 1990. – 580 p.
24. CopelandLee. A Practitioner's Guide to Software Test Design. – Artech House, 2004. – 300 p.
25. Desai S., Srivastava A. Software testing: a practical approach. – PHI Learning Pvt. Ltd., 2012. – 192 p.

References:

1. Barsukov V. S. Bezopasnost': tekhnologii, sredstva, uslugi. – М. : KUDITS – OBRAZ, 2001. – 496 s. [Barsukov V. S. Security: technology, tools, services. – М. : KUDITS – IMAGE, 2001. – 496 p. (In Russ.).]
2. Gafner V. V. Informatsionnaya bezopasnost': Uchebnoye posobiye.– Rostov na Donu. : Feniks, 2010. – 324 s. [Gafner V. Information Security: Study Guide. – Rostov on Don. : Phoenix, 2010. – 324 p. (In Russ.).]
3. Gromov YU. YU. Informatsionnaya bezopasnost' i zashchita informatsii: Uchebnoye posobiye.– St. Oskol : TNT, 2010. – 384 s. [Gromov Yu. Yu. Information Security and Information Security: tutorial. – Art. Oskol: TNT, 2010. – 384 p. (In Russ.).]
4. Okhrana truda i promyshlennaya okhrana. [Elektronnyy resurs]. URL: <http://prom-nadzor.ru> (data obrashcheniya 25.05.2019) [Labor and industrial safety. [Electronic resource]. URL: <http://prom-nadzor.ru> (access date 25.05.2019) (In Russ.).]
5. GOST R 54831-2011 Sistemy kontrolya i upravleniya dostupom. Ustroystva pregrazhdayushchiye upravlyayemye. Obshchiye tekhnicheskiye trebovaniya. Metody ispytaniy. – М. : Standartinform, 2012. – 16 s. [GOST R 54831-2011 Access Control Systems. Devices blocking managed. General technical requirements. Test methods. - М. : Standardinform, 2012. – 16 p. (In Russ.).]
6. Badikov A. V., Bondarev P. V. Sistemy kontrolya i upravleniya dostupom. Laboratornyy praktikum. – М. : NIYAU MIFI, 2010. – 128 s. [Badikov A. V., Bondarev P. V. Access control and management systems. Laboratory workshop. - М. : NRNU MEPhI, 2010. – 128 p. (In Russ.).]
7. Volkhonskiy V. V. Nekotoryye voprosy razrabotki metodologii postroyeniya sistem kontrolya dostupa i vybora tekhnologii identifikatsii // Informatsionno-upravlyayushchiye sistemy. – 2012. – № 4. – с. 78-83. [Volkhonsky V. V. Some issues of developing a methodology for building access control systems and the choice of identification technology // Information Management Systems. – 2012. – № 4. - p. 78–83. (In Russ.).]
8. Volkhonskiy V. V. Sistemy kontrolya i upravleniya dostupom.– SPb. : Universitet ITMO, 2015. – 200 s. [Volkhonsky V. V. Access control and management systems. – SPb. : ITMO University, 2015. – 200 p. (In Russ.).]
9. Vorona V. A., Tikhonov V. A. Sistemy kontrolya i upravleniya dostupom. – М. : Goryachaya liniya-Telekom, 2010. – 272 s. [Vorona V. A., Tikhonov V. A. Access control systems. – М. : Hotline-Telecom, 2010. – 272 p. (In Russ.).]
10. Schityvatel' beskontaktnyy PERCo-IR03. Rukovodstvo po ekspluatatsii. [Elektronnyy resurs]. URL: http://www.etk-elcom.ru/docs/PERCo_IR03D_Rukovodstvo_po_ekspluatatsii.pdf (data obrashcheniya 25.05.2019). [Reader non-contact PERCo-IR03. Manual. [Electronic resource]. URL: http://www.etk-elcom.ru/docs/PERCo_IR03D_Rukovodstvo_po_ekspluatatsii.pdf (access date 25.05.2019) (In Russ.).]

11. Kayumova A. V. Vizual'noye modelirovaniye sistem v StarUML: uchebnoye posobiye.– Kazan' : Kazanskiy federal'nyy universitet, 2013. – 104 s. [Kayumova A. V. Visual systems modeling in StarUML: study guide. – Kazan : Kazan Federal University, 2013. – 104 p. (In Russ.)].
12. Daoust N. UML Requirements Modeling For Business Analysts: Steps to Modeling Success. Technics Publications, 2012. – 268 p.
13. Internet-sayt Arduino.ru. [Elektronnyy resurs]. URL: <http://arduino.ru> (data obrashcheniya 25.05.2019). [Internet site Arduino.ru. [Electronic resource]. URL: <http://arduino.ru> (access date 25.05.2019) (In Russ.)].
14. Arduino. [Электронный ресурс]. URL: <https://www.arduino.cc/> (access date 25.05.2019).
15. Margolis M. Arduino Cookbook. O'Reilly Media, Inc., 2011. – 662 p.
16. Sommer Ul. Programirovaniye mikrokontrollernykh plat Arduino/Freeduino. SPb. : BKHV-Peterburg, 2017. 240 s. [Sommer Str. Arduino / Freeduino microcontroller programming. SPb. : BHV-Petersburg, 2017. 240 p. (In Russ.)].
17. GOST 2.701-2008. Yedinaya sistema konstruktorskoy dokumentatsii. Skhemy. Vidy i tipy. Obshchiye trebovaniya k vypolneniyu. M. : Standartinform. 2009. – 16 s. [GOST 2.701-2008. Unified system for design documentation. Scheme. Types and types. General requirements for implementation. M. : Standardinform. 2009. – 16 p. (In Russ.)].
18. Petin V. A. Projekty s ispol'zovaniyem kontrollera Arduino. – SPb. : BKHV-Peterburg, 2019. – 496 s. [Petin V. A. Projects using the Arduino controller. – SPb. : BHV-Petersburg, 2019. 496 p. (In Russ.)].
19. Birman I. Pol'zovatel'skiy interfeys. – M. : Dizayn-byuro Artoma Gorbunova, 2017. 363 s. [Birman I. User interface. M. : Artyom Gorbunov design bureau, 2017. 363 p. (In Russ.)].
20. Kuznetsov S. D. Osnovy baz dannykh. – M. : Internet-universitet informatsionnykh tekhnologiy; BINOM. Laboratoriya znaniy, 2007. 484 s. [Kuznetsov S. D., Basics of Databases. M. : Internet University of Information Technology; BINOMIAL. Laboratory of Knowledge, 2007. 484 p. (In Russ.)].
21. Kulikov S. Testirovaniye programmnoy obespecheniya. Bazovyy kurs.– Minsk : Chetyre chetverti, 2017. – 312 s. [Kulikov S. Software testing, Basic course – Minsk : Four quarters, 2017. – 312 p. (In Russ.)].
22. Beyzer B. Testirovaniye chernogo yashchika. Tekhnologii funktsional'nogo testirovaniya programmnoy obespecheniya i sistem. – SPb. : Izdatel'skiy Dom Piter, 2004. 321 s. [Beizer B. Testing of the black box. Technology functional testing software and systems. – SPb. : Publishing House Peter, 2004. – 321 p. (In Russ.)].
23. Beizer B. Software Testing Techniques. Itp – Media, 1990. 580 p.
24. CopelandLee. A Practitioner's Guide to Software Test Design. Artech House, 2004. 300 p.
25. Desai S., Srivastava A. Software testing: a practical approach. PHI Learning Pvt. Ltd., 2012. 192 p.

Сведения об авторах:

Бужинская Надежда Владимировна - кандидат педагогических наук, доцент, кафедра информационных технологий.

Васева Елена Сергеевна - кандидат педагогических наук, доцент, кафедра информационных технологий.

Искандаров Рустам Наильевич - ведущий специалист.

Шубина Наталья Валерьевна - кандидат технических наук, доцент, кафедра информационных технологий.

Information about the authors:

Nadezhda V. Buzhinskaya - Cand. Sc. (Pedagogical), Assoc. Prof., Department of Information Technology.

Elena S. Vaseva - Cand. Sc. (Pedagogical), Assoc. Prof., Department of Information Technology.

Rustam N. Iskandarov - Leading Specialist.

Natalya V. Shubina - Cand. Sc. (Technical), Assoc. Prof., Department of Information Technology.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest.

The authors declare no conflict of interest.

Поступила в редакцию 14.02.2019.

Received 14.02.2019.

Принята в печать 22.03.2019.

Accepted for publication 22.03.2019.