

М.Д. Бурмистров,  
С.А. Кошелева,  
И.Е. Пестов,  
П.С. Шинкарева

## Разработка программно-аппаратной системы контроля и управления доступом

*В данной статье ставится задача разработать программно-аппаратную систему контроля и управления доступом на основе аппаратных платформ Arduino Uno и Raspberry Pi. Разработанная программно-аппаратная система предназначена для сбора данных и хранения их в базе. Представленный комплекс можно переносить и использовать в любом месте, что объясняет его высокую мобильность.*

**Ключевые слова:** Arduino, Raspberry Pi, RFID, NFC, информационная безопасность, система контроля и управления доступом.

M.D. Burmistrov,  
S.A. Kosheleva,  
I.E. Pestov,  
P.S. Shinkareva

## Development of hardware and software system for access control and management

*This article aims to develop a hardware-software system for access control and management based on the hardware platforms Arduino Uno and Raspberry Pi. The developed software and hardware system is designed to collect data and store them in the database. The presented complex can be carried and used anywhere, which explains its high mobility.*

**Keywords:** Arduino, Raspberry Pi, RFID, NFC, information security, access control system.

### Введение

Проблема сбора, хранения и обработки больших объёмов данных в настоящее время стоит наиболее остро. С развитием Интернета человечество получило доступ к информации со всего Земного шара; количество уникальных пользователей Всемирной сети растёт стремительными темпами, равно как и техническая оснащённость различных организаций и предприятий. Современные методы ведения коммерческой, учебной и других видов деятельности всё чаще и чаще включают в себя использование информационных технологий. В каждой из сфер деятельности непременно задействованы люди – а, как известно, самой серьёзной уязвимостью в любой системе безопасности является человек – и чтобы избежать несанкционированного доступа каждому пользователю необходимо пройти процедуры регистрации в информационной системе – аутентификацию и идентификацию. Для этой цели в организациях внедряются системы контроля и управления доступом.

### Постановка задачи

Необходимо спроектировать и разработать устройство системы контроля и управления доступом на базе устройств Raspberry Pi и Arduino Uno. Устройство должно иметь модуль ввода данных и систему хранения этих данных. Ввод данных должен осуществляться посредством бесконтактного считывания информации со смарт-карты. Хранение должно осуществляться при помощи программного обеспечения Raspberry Pi. Также система должна иметь графический пользовательский интерфейс для просмотра и отслеживания введенной информации: веб-приложение, имеющее серверную часть, взаимодействующую с базой данных и обслуживающую клиентские запросы. Приложение, равно как и операционная система устройства, должно быть защищено от распространенных угроз безопасности информационных систем [5].

Для реализации проекта были использованы устройства: Arduino Uno, Raspberry Pi 3, RFID/NFC модуль.

**Raspberry Pi 3** – это полноценный компьютер с 64-х битным четырехъядерным процессором ARM Cortex-A53 на однокристальном чипе Broadcom BCM2837 [9]. Основной операционной системой является Linux [6].

Плата **Arduino Uno**–платформа для разработки на базе микроконтроллера ATmega328P [8]. Имеет 14 цифровых и 6 аналоговых пинов для подключения разнообразных датчиков, светодиодов и других внешних устройств.

**RFID** – беспроводное бесконтактное использование радиочастотных волн для передачи данных [10].

Схема соединений устройств представлена на рисунке 1. RFID/NFC-считыватель соединяется с Arduino для передачи данных с NFC-метки, для соединения используются три трехпиновых шлейфа. Затем Arduino соединяется с Raspberry Pi посредством USB-кабеля для дальнейшей передачи считанных данных через последовательный интерфейс.

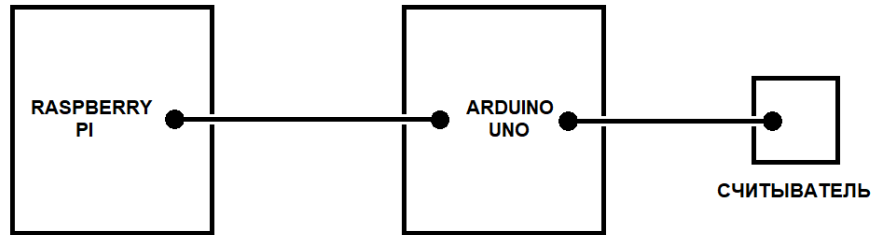


Рис. 1. Схема соединения устройств

**Программная часть устройства** включает в себя:

1. Программу для Arduino, принимающую данные со считывателя и передающую их на Raspberry Pi;
2. База данных, хранящая считанные данные;
3. Скрипт, принимающий данные, передаваемые с Arduino, и пополняющий ими базу данных;
4. Веб-приложение, соединенное с базой данных, предоставляющее доступ к записям в базе данных.

### Программа для Arduino

Для взаимодействия со считывателем используется библиотека Adafruit PN532. К Raspberry Pi для передачи данных Arduino подключается с помощью USB-кабеля, программа использует последовательный интерфейс обмена данными. Реализация программы представлена на листинге 1.

Листинг 1.

```
Adafruit_PN532 nfc(PN532_IRQ, 100);
void setup(void) {
  Serial.begin(9600);
  nfc.begin();
  int versiondata = nfc.getFirmwareVersion();
  if (!versiondata) {
    while(1) {}
  }
  nfc.SAMConfig();
```

```
}
void loop(void)
{
  uint8_t success;
  uint8_t uid[8];
  uint8_t uidLength;
  success =
  nfc.readPassiveTargetID(PN532_MIFARE_ISO1443A, uid, &uidLength);
  if (success) {
    nfc.PrintHex(uid, uidLength);
    Serial.println("");
    delay(1000);
  }
}
```

### База данных

Для хранения данных используется реляционная СУБД MySQL. В базе данных создана таблица, имеющая структуру, описанную в табл. 1.

Таблица 1. Структура таблицы записей

Название столбца	Тип столбца
id	INT
data	VARCHAR(255)
time	DATETIME

Таким образом, каждая запись имеет уникальный идентификатор, считанные данные карты и время создания записи. Скрипт, описывающий модель таблиц в базе данных в виде классов языка Python представлен в листинге 2.

Листинг 2.

```
db = peewee.MySQLDatabase('raspdb', user='www', password='www')
class User(peewee.Model):
    username = peewee.CharField(unique=True)
    password = peewee.CharField(default='')
class Meta:
    database = db
class Record(peewee.Model):
    data = peewee.TextField()
    time = peewee.DateTimeField(default=datetime.now)
class Meta:
    database = db
```

**Считывающий скрипт**

Для взаимодействия с USB-портом через последовательный интерфейс используется модуль pyserial. При помощи данного модуля производится прием и разбор данных, затем производится добавление записи в базу данных. Соединение с базой данных происходит при помощи модуля рееее. Код скрипта представлен на листинге 3.

Листинг 3.

```
serial = pyserial.Serial('/dev/ttyACM0', 9600)
while True:
    line = serial.readline()
    if line:
        line = line.decode('utf-8')
        db.Record.create(data=line, time=datetime.now())
```

**Веб-приложение**

Веб-приложение реализуется на основе фреймворка Flask. Взаимодействие с базой данных также происходит при помощи модуля рееее.

В целях обеспечения безопасности веб-интерфейса [4] в приложении реализован механизм защиты от несанкционированного доступа путем идентификации и аутентификации пользователя по логину и паролю, а также защита от таких актуальных угроз, как прослушивание канала связи атакой «человек посредине» [7].

На уровне ОС с использованием метода, изложенного в [2], реализована защита от угроз типа rootkit.

Код приложения представлен на листинге 4.

Листинг 4.

```
context = SSL.Context(SSL.TLSv1_2_METHOD)
context.use_privatekey_file('server.key')
context.use_certificate_file('server.crt')
app = Flask(__name__)
bcrypt = Bcrypt(app)
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        if not 'username' in request.form or not 'password' in request.form:
            return render_template('login.html')
        user = db.User.get_or_none(username=request.form['username'])
        if user is None or not bcrypt.check_password_hash(user.password, request.form['password']):
            return render_template('login.html')
        session['username'] = user.username
        return redirect(url_for('index'))
        return render_template('login.html')
```

Таким образом, как показано на рисунке 2, считывая данные со смарт-карты, скрипт, слушающий последовательный порт, снабжает базу данных записями, которые в свою очередь, получает веб-приложение, которое затем отображает данные записи в виде HTML-страницы.

На рисунке 3 представлено собранное переносное устройство.

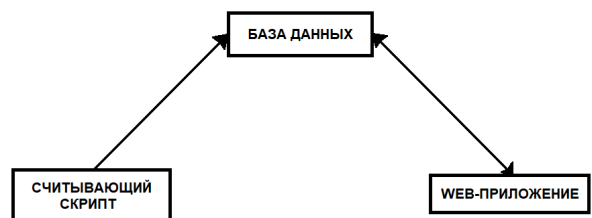


Рис. 2. Схема взаимодействия программных элементов на базе Raspberry Pi

Представленное на рисунке 3 устройство является рабочей системой контроля и управления доступом. В дополнение к этому, устройство защищено от некоторых актуальных угроз безопасности. Тем не менее, многие уяз-

вимости остаются открытыми, поэтому в долгосрочной перспективе целесообразно провести аудит и устранить выявленные слабые места системы [3]. Дальнейшей задачей является рассмотрение методов устранения уязвимостей [1].

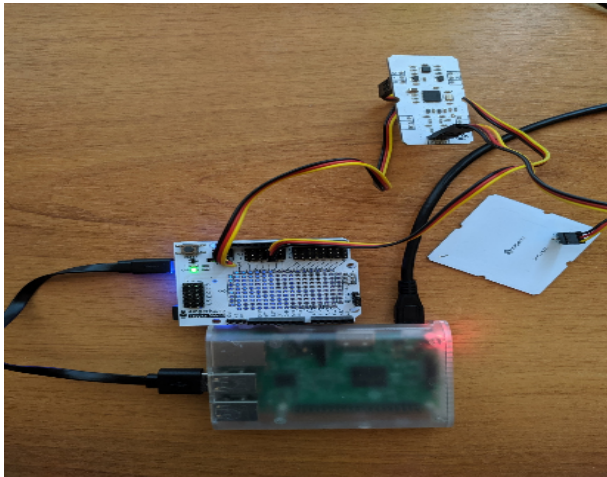


Рис. 3. Собранное устройство

### Заключение

Разработанное устройство протестировано

### СПИСОК ЛИТЕРАТУРЫ

1. Аверченков, В.И. Междисциплинарные аспекты анализа тенденций развития интернета вещей (обзор российских и зарубежных исследований) / В.И. Аверченков, К.В. Герасимов, Н.А. Слесаренко // Эргодизайн. – 2019. - №3(05). – С. 106-114. DOI: 10.30987/article\_5d25e4dcc73a24.98125589.
2. Кирилова, К.С. Анализ существующих методов реализации rootkit / К.С. Кирилова, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 492–497.
3. Пестов, И.Е. Выявление угроз безопасности информационных систем / И.Е. Пестов, Д.В. Сахаров, И.Ю. Сергеева, И.С. Чернобородов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2017. С. 525–527.
4. Таргонская, А.И. Разработка защищенного веб-интерфейса для управления устройствами в сети / А.И. Таргонская, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2019.

на практике. Малые размеры и масса используемых элементов позволяют легко перенести устройство, тем самым давая возможность развернуть портативную считывающую станцию для организации сбора и учета данных в любом месте, в отличие от других систем контроля и управления доступом.

Аппаратная часть комплекса включает в себя вышеупомянутые устройства Arduino Uno и Raspberry Pi 3, а также RFID/NFC-считыватель. Последний подключается к Arduino Uno и передает данные по протоколу I<sup>2</sup>C. Arduino Uno, в свою очередь, соединяется с Raspberry Pi 3 посредством USB-кабеля и передает данные через последовательный интерфейс передачи данных.

Программная часть комплекса включает в себя исполняемый код, загружаемый в Arduino Uno, скрипт на языке программирования Python для считывания данных, передаваемых с Arduino Uno на Raspberry Pi 3, и помещения их в базу данных, непосредственно базу данных, хранящую данные, и веб-приложение также на языке Python, предоставляющее удобный графический интерфейс пользователя для просмотра хранимых данных в базе данных.

### REFERENCES

1. Averchenkov, V. I. Interdisciplinary aspects of trends' analysis in the development of the Internet of things (review of Russian and foreign studies) / V.I. Averchenkov, K.V. Gerasimov, N.A. Slesarenko // Ergodizayn. – 2019. - No. 3 (05). - P. 106-114. DOI: 10.30987/article\_5d25e4dcc73a24.98125589.
2. Kirilova, K.S. Analysis of existing methods for implementing rootkit / K.S. Kirilova, A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VIII international scientific-technical and scientific-methodical conference: sat.nauch. - St. Petersburg. : SPbSTU, 2019. - P. 492-497.
3. Pestov, I E. Identification of security threats to information systems / I E. Pestov, D.V. Sakharov, I.Yu. Sergeeva, I.S. Chernoborodov // Actual problems of infotelecommunications in science and education. VIII international scientific-technical and scientific-methodical conference: sat.nauch. - St. Petersburg.: SPbSTU, 2017. - P. 525-527.
4. Targonskaya, A.I. Development of a secure web interface for managing devices in the network / A.I. Targonskaya, A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VIII international scientific-technical and scientific-methodical conference: sat.nauch. - St. Petersburg.: SPbSTU, 2019. - P. 734-739.

С. 734–739.

5. Темченко, В.И. Проектирование модели информационной безопасности в операционной системе / В.И. Темченко, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 740–745.

6. Цветков, А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux / А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657–662.

7. Цветков А.Ю. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ / А.Ю. Цветков, М.Е. Шалаева, М.А. Юрченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 756–761.

8. Arduino Reference [Электронный ресурс]. URL: <https://www.arduino.cc/reference/en/> (дата обращения 02.12.2019).

9. Raspberry Pi 3 Model B [Электронный ресурс]. URL: <https://www.raspberrypi.org/products/raspberry-pi-3-model-b/> (дата обращения 02.12.2019).

10. RFID/NFC-сканер [Амперка / Вики] [Электронный ресурс]. URL: <http://wiki.amperka.ru/продукты:nfc> (дата обращения 02.12.2019).

5. Temchenko, V.I. Designing an information security model in an operating system / V.I. Temchenko, A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VIII international scientific-technical and scientific-methodical conference: sat.nauch. - St. Petersburg.: SPbSTU, 2019. - P. 740-745.

6. Tsvetkov, A.Yu. Research of existing mechanisms of protection of operating systems of the Linux family / A.Yu. Tsvetkov // Actual problems of infotelecommunications in science and education. VII international scientific-technical and scientific-methodical conference: sat.nauch. article. - SPb.: SPbSTU, 2018. - P. 657-662.

7. Tsvetkov, A.Yu. Providing security in a client-server Java application for accounting and automatic verification of laboratory work / A.Yu. Tsvetkov, M.E. Shalaeva, M.A. Yurchenko // Actual problems of infotelecommunications in science and education. VIII international scientific-technical and scientific-methodical conference: sat.nauch. - St. Petersburg.: SPbSTU, 2019. - P. 756-761.

8. The Arduino Reference [Electronic resource]. URL: <https://www.arduino.cc/reference/en/> (accessed 02.12.2019).

9. Raspberry Pi 3 Model B [Electronic resource]. URL: <https://www.raspberrypi.org/products/raspberry-pi-3-model-b/> (accessed 02.12.2019).

10. RFID / NFC scanner [Amperka / Wiki] [Electronic resource]. URL: <http://wiki.amperka.ru/продукты:nfc> (accessed 02.12.2019).

Ссылка для цитирования:

Бурмистров, М.Д. Разработка программно-аппаратной системы контроля и управления доступом / М.Д. Бурмистров, С.А. Кошелева, И.Е. Пестов, П.С. Шинкарева // Эргодизайн. – 2020. - №1 (07). – С. 19-24. DOI: 10.30987/2658-4026-2020-1-19-24.

**Сведения об авторах:**

**Пестов Игорь Евгеньевич**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,  
г. Санкт-Петербург  
старший преподаватель  
Тел.: +79313062628  
E-mail: [ip@sut.ru](mailto:ip@sut.ru)  
ORCID 0000-0001-6801-9777

**Шинкарева Полина Сергеевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича  
г. Санкт-Петербург  
студентка  
Тел.: +79992314612  
E-mail: [kampollyy@gmail.com](mailto:kampollyy@gmail.com)  
ORCID 0000-0003-0946-1631

**Кошелева Софья Андреевна**

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,

**Abstracts:**

**I.E. Pestov**

Saint-Petersburg state University of telecommunications them. Prof. M. A. Bonch-Bruevich  
Saint Petersburg  
senior lecturer  
Tel.: +79313062628  
E-mail: [ip@sut.ru](mailto:ip@sut.ru)  
ORCID 0000-0001-6801-9777

**P.S. Shinkareva**

Saint Petersburg state University of telecommunications.  
Prof. M. A. Bonch-Bruevich  
Saint Petersburg  
student  
Tel.: +79992314612  
E-mail: [kampollyy@gmail.com](mailto:kampollyy@gmail.com)  
ORCID 0000-0003-0946-1631

**S.A. Kosheleva**

Saint Petersburg state University of telecommunications.  
Prof. M. A. Bonch-Bruevich

г. Санкт-Петербург  
студентка  
Тел.: +79094605040  
E-mail: [koshelevason@yandex.ru](mailto:koshelevason@yandex.ru)  
ORCID 0000-0002-3475-9168

**Бурмистров Максим Дмитриевич**  
Санкт-Петербургский государственный университет  
телекоммуникаций им. проф. М.А. Бонч-Бруевича,  
г. Санкт-Петербург  
студент  
Тел.: +79995343827  
E-mail: [burmistrovm@live.ru](mailto:burmistrovm@live.ru)  
ORCID 0000-0002-9372-060X

Saint Petersburg  
student  
Tel.: +79094605040,  
E-mail: [koshelevason@yandex.ru](mailto:koshelevason@yandex.ru)  
ORCID 0000-0002-3475-9168

**M.D. Burmistrov**  
Saint Petersburg state University of telecommunications.  
Prof. M. A. Bonch-Bruevich  
Saint Petersburg  
student  
Tel.: +79995343827  
E-mail: [burmistrovm@live.ru](mailto:burmistrovm@live.ru)  
ORCID 0000-0002-9372-060X

Статья поступила в редколлегию 02.02.2020 г.

Рецензент:

д-р техн. наук., профессор  
Брянского государственного  
технического университета,  
член редсовета журнала «Эргодизайн»

Авенченков В.И.

Статья принята к публикации 14.02.2020 г.