УДК 004.93'1

СИСТЕМА УПРАВЛЕНИЯ АУТЕНТИФИКАЦИЕЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ СКУД

Иванов А.П., Кисель А.В.

гр.161402

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С. – доцент кафедры ЗИ, кандидат технических наук, доцент.

Аннотация. В материалах доклада представлены результаты разработки и тестирования системы контроля и управления доступом на основе RFID-карты и

биометрической аутентификации, интегрированной с Keycloak. Данная система может использоваться для обучения студентов различных специальностей, включая 6-05-0611-02 «Информационная безопасность», для повышения их навыков в области информационной безопасности.

Ключевые слова: СКУД, RFID-карта, биометрическая аутентификация, Keycloak.

Введение. С развитием информационных технологий и ростом количества цифровых ресурсов обеспечение надежной аутентификации пользователей становится критически важной задачей. Традиционные методы, основанные только на парольной защите, не всегда обеспечивают достаточный уровень безопасности, особенно в крупных организациях. В связи с этим активно развивается многофакторной аутентификации, которая сочетает несколько уровней проверки пользователя.

Одним из эффективных решений является интеграция систем контроля и управления доступом с централизованными механизмами аутентификации. В такой системе пользователь сначала проходит проверку по RFID-карте, затем подтверждает личность с помощью биометрии, после чего данные передаются в систему управления доступом и аутентификацией, такую как Keycloak. На основании полученной информации происходит автоматическая разблокировка учетной записи и предоставление доступа к информационным ресурсам.

Актуальность данного подхода обусловлена ростом числа киберугроз, связанных с компрометацией учетных данных и несанкционированным доступом. Использование такой системы позволяет значительно повысить уровень безопасности, минимизировать риски несанкционированного доступа и обеспечить надежный контроль как за физическим объектам, так и за информационными ресурсами.

Цель данной научной работы заключается в разработке и реализации СКУД с интеграцией механизмов многофакторной аутентификации и управления учетными записями. Полученные результаты могут стать основой для создания безопасных и эффективных решений по защите корпоративных и государственных информационных ресурсов.

Основная часть. Для обеспечения надежной аутентификации пользователей и защиты информационных ресурсов была разработана система контроля и управления доступом с многофакторной аутентификацией. Основной задачей системы является повышение уровня безопасности и исключение несанкционированного доступа за счет использования RFID-карт и биометрической аутентификации, а также интеграции с системой управления учетными записями для централизованного контроля доступа.

Для эффективной работы системы была разработана четкая последовательность действий, которая начинается с идентификации пользователя через RFID-карту, затем выполняется биометрическая аутентификация, и только после этого осуществляется проверка учетной записи через систему Keycloak. Эта последовательность обеспечивает надежную защиту на каждом этапе процесса. На рисунке 1 представлена блок-схема, описывающая функционирование СКУД, а на рисунке 2 – блок-схема, описывающая функционирование система управления доступом и аутентификацией – Keycloak.

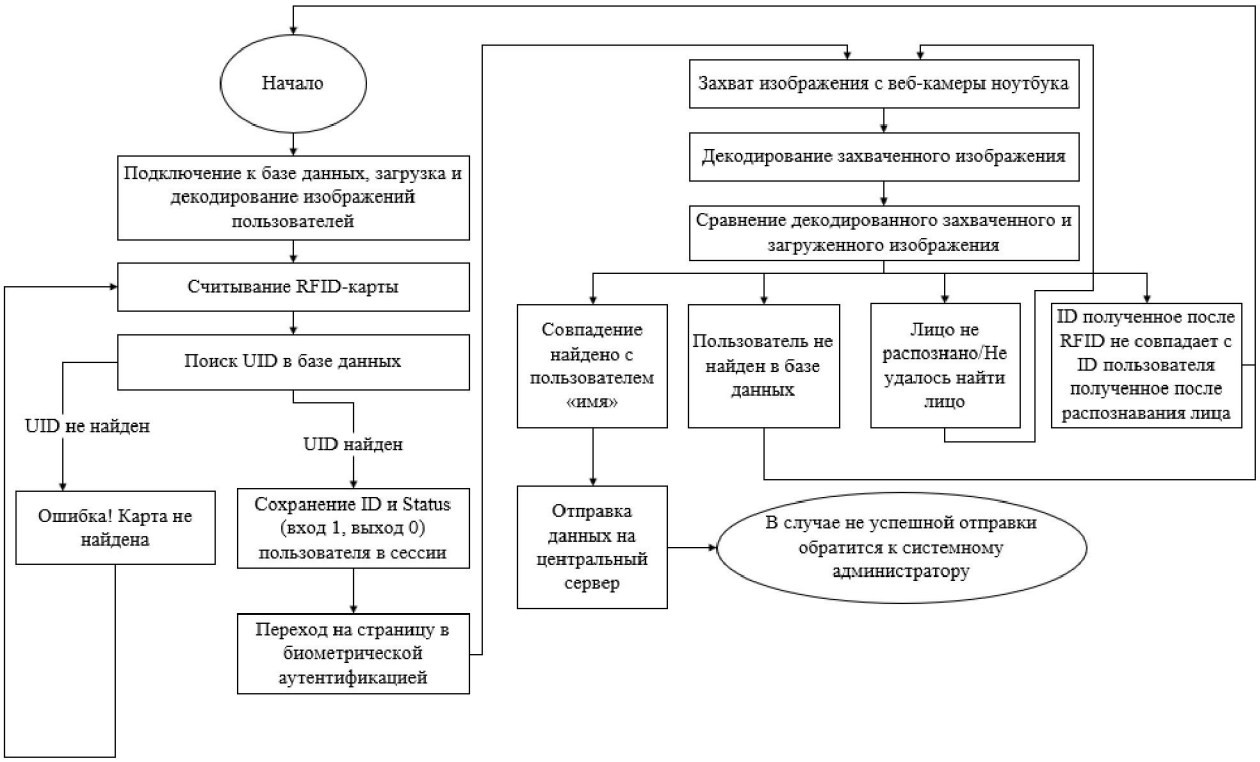

Рисунок 1 – Блок-схема функционирования СКУД

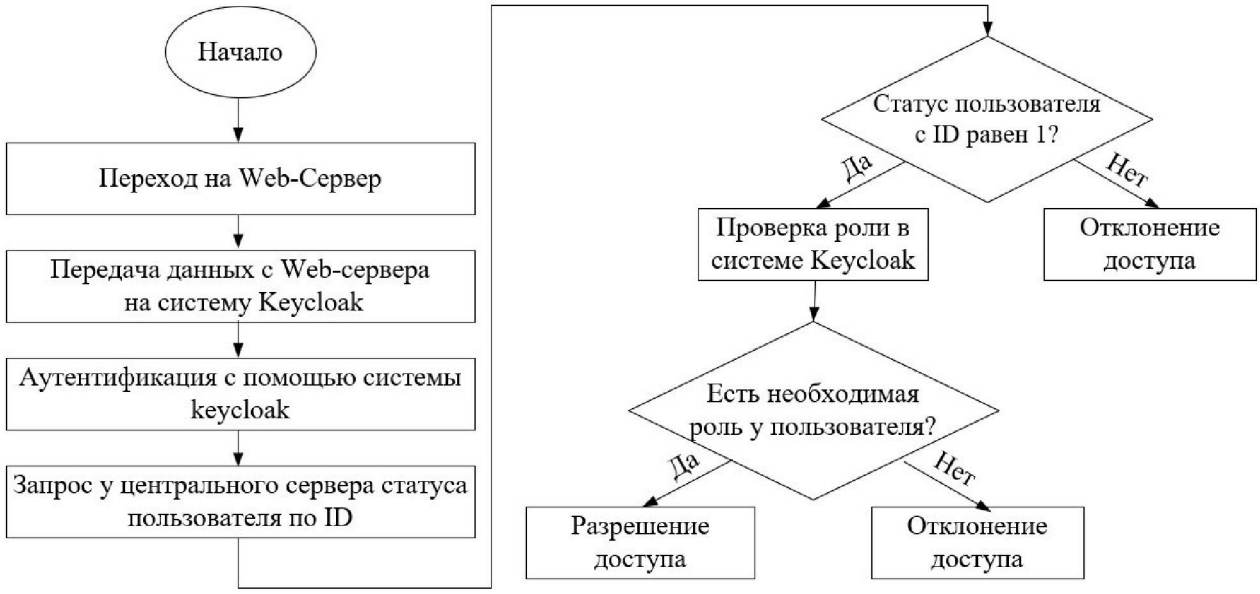

Рисунок 2 – Блок-схема функционирования Keycloak

В процессе тестирования системы были проведены различные сценарии, включая успешный вход с RFID-картой и биометрическими данными, а также отказ в доступе при несоответствии биометрических данных или использовании незарегистрированной карты. Все этапы аутентификации были проверены на корректность работы, и система показала высокую степень надежности. Результаты тестирования подтверждают, что система эффективно предотвращает несанкционированный доступ и минимизирует риски компрометации учетных

данных.

Разработанная система может быть дополнительно усилена следующими мерами:

1 Журналирование событий – ведение логов всех попыток входа, что позволяет своевременно выявлять подозрительную активность.

2 Мониторинг в реальном времени – отображение информации о пользователях, которые зашли в здании или вышли из него.

3 Интеграция с системой управления инцидентами – для повышения уровня безопасности можно внедрить систему, которая будет автоматически реагировать на подозрительные события, отправляя уведомления систему администратору.

Заключение. В ходе разработки была создана эффективная система контроля и управления доступом, сочетающая RFID, биометрическую аутентификацию и интеграцию с Keycloak для управления учетными записями. Тестирование подтвердило ее высокую надежность и защиту от несанкционированного доступа. Перспективы дальнейшего развития включают интеграцию дополнительных методов защиты, таких как журналирование событий, мониторинг в реальном времени и расширение функциональности. Такая система может быть внедрена в учебные процессы для студентов различных специальностей, включая 1-98 01 02 «Защита информации в телекоммуникациях».

Список литературы

1. MFRC522 [Электронный ресурс]. Режим доступа: https://github.com/miguelbalboa/rfid?ysclid=m82qd1ku2p160266956. – Дата доступа: 11.02.2025.

2. Server Administration Guide [Электронный ресурс]. Режим доступа: https://www.keycloak.org/docs/latest/server_admin/index.html. – Дата доступа: 24.02.2025.

3. Flask's documentation [Электронный ресурс]. Режим доступа: https://flask.palletsprojects.com/en/stable/. – Дата доступа: 01.03.2025.

UDC 004.93'1

USER AUTHENTICATION MANAGEMENT SYSTEM FOR INFORMATION RESOURCES USING ACCESS CONTROL SYSTEMS

Ivanov A.P., Kisel A.V.

gr.161402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department

Annotation. The report presents the results of the development and testing of an access control system based on RFID cards and biometric authentication, integrated with Keycloak. This system can be used for training students of various specialties, including 6-05-0611-02 "Information Security," to enhance their skills in information security.

Keywords: ACS, RFID card, biometric authentication, Keycloak.