DOI: 10.18137/RNU.V9187.22.02.P.043 УДК 004.056

К.Е. Буяков, Д.А. Елизаров, М.Я. Епифанцева, Т.А. Мызникова, А.В. Шилер

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ДАННЫХ

Аннотация. Рассмотрены особенности современной архитектуры систем контроля и управления доступом, лучшие практики и тренды в области обеспечения безопасности посредством системы контроля и управления доступом, а также их основные характеристики. Доказана актуальность разработки программно-аппаратного комплекса контроля доступа с использованием биометрической системы аутентификации, основанной на распознавании отпечатков пальцев. Разработанная система обеспечивает гибкую интеграцию с корпоративными сервисами организации.

Ключевые слова: система контроля и управления доступом, обеспечение информационной безопасности, управление доступом, биометрическая аутентификация, отпечаток пальца, смартфон.

K.E. Buyakov, D.A. Elizarov, M.Ya. Epifanceva, T.A. Myznikova, A.V. Shiler

DEVELOPMENT OF BIOMETRIC ACCESS CONTROL SYSTEM

Abstract. The article discusses the features of the modern architecture of access control systems, best practices and trends in the field of security, as well as the main characteristics. The relevance of the development of a software and hardware complex for access control using a biometric authentication system based on fingerprint recognition. The developed system provides flexible integration with corporate services of the organization.

Keywords: access control systems, information security, access control, biometric authentication, fingerprint, Smartphone.

Введение

Согласно [4; 5] система контроля и управления доступом (далее – СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью. Сегодня СКУД широко применяется как дополнение к существующим системам защиты и охраны и представляет собой самое интенсивно развивающееся направление в технике обеспечения информационной безопасности (далее – ИБ). Интеграция систем СКУД и ИБ позволяет построить корпоративную информационную систему с учетом ограничений или запрета доступа к информационным ресурсам предприятия, автоматически блокировать персональный компьютер в зависимости от местонахождения пользователя. Повышенные требования к функционалу СКУД благоприятно влияют на появление эффективных и оптимальных технических решений для создания комплексной системы безопасности.

Стоит отметить, что в настоящее время СКУД является одним из наиболее развитых сегментов рынка ИБ как в России, так и за рубежом. По результатам проведенного компанией Marketsand Markets исследования, глобальный рынок контроля доступа к 2024 году вырастет более чем на 60 %. Мировой рынок контроля доступа в денежном выражении увеличится с 7,5 млрд долларов в 2018 году до 12,1 млрд долларов к 2024 году. Аналитики Research and Markets считают, что мировой рынок контроля доступа вырастет с 8,6 млрд

Буяков Кирилл Евгеньевич
старший разработчик. ООО «МТС «Диджитал», Москва. Сфера научных интересов: разработка и верификация программного обеспечения. Автор 2 опубликованных научных работ.
Электронный адрес: buyakov_98@bk.ru

ЕлизаровДмитрийАлександрович
кандидат технических наук, доцент. Омский государственный университет путей сообщения, город Омск. Сфера научных интересов: разработка и верификация программного обеспечения; вопросы обеспечения информационной безопасности. Автор более 50 опубликованных научных работ.
Электронный адрес: elizarovdaib@gmail.com

Епифанцева Маргарита Ярополковна
кандидат технических наук, доцент. Омский государственный университет путей сообщения, город Омск. Сфера научных интересов: теория вероятностей и математическая статистика; численные методы; разработка автоматизированных систем. Автор более 10 опубликованных научных работ.
Электронный адрес: mepifanceva@gmail.com

Мызникова Татьяна Александровна
кандидат технических наук, доцент. Омский государственный университет путей сообщения, город Омск. Сфера научных интересов: защита информации встроенными средствами операционных систем. Автор более 20 опубликованных научных работ.
Электронный адрес: tmyzn@mail.ru

Шилер Александр Валерьевич
доктор технических наук, профессор. Омский государственный университет путей сообщения, город Омск. Сфера научных интересов: искусственный интеллект; разработка интеллектуальных приложений; динамические системы; техническая защита информации. Автор 90 опубликованных научных работ.
Электронный адрес: shiler_alex@inbox.ru

долларов США в 2020 году до 12,8 млрд долларов США к 2025 году при среднегодовом темпе роста 8,2 % [1].

В [7] описаны лучшие практики и тренды в области обеспечения безопасности посредством СКУД. Имеющиеся сейчас на предприятиях СКУД не могут интегрироваться с внешними системами безопасности, хотя современные СКУД должны обеспечивать интеграцию с другими системами безопасности и логистическими процессами предприятия (транспорт, посетители, разовые и временные пропуска), кадровыми системами, а также обеспечивать в качестве способа идентификации применение биометрических данных. Гибкость разрабатываемой СКУД должна способствовать дальнейшему увеличению функционала и расширению возможностей, уменьшению использования вспомогательного оборудования, использованию контроллеров, работающих по протоколу Ethernet, универсальных контроллеров с встроенными считывателями карт доступа с поддержкой биометрической идентификации.

Схема гибкой архитектуры СКУД представлена на Рисунке 1 [2; 8].

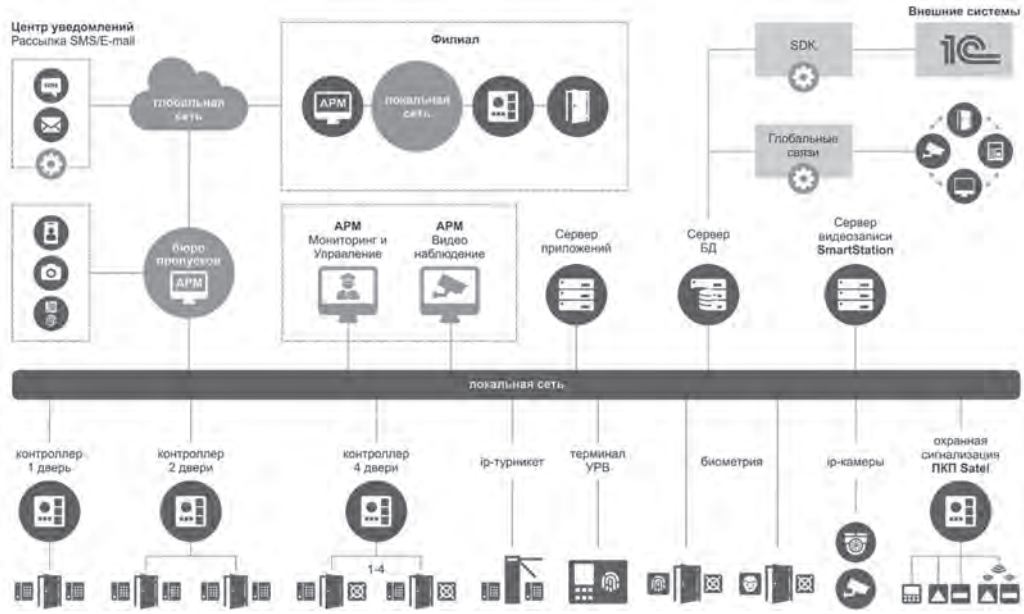

Рисунок 1. Схема гибкой архитектуры СКУД

Тремя ключевыми трендами современных СКУД являются: 1) развитие технологий мобильного доступа, 2) рост популярности IP-контроллеров и электронных замков, 3) усиление роли биометрической идентификации. ***Биометрическая идентификация*** – один из наиболее надежных и эффективных инструментов для организации СКУД на объектах с повышенными требованиями безопасности [9]. Биометрия – одна из самых быстрорастущих технологий, используемых для защиты периметра [6]. СКУД, основанная на распознавании отпечатков пальцев, продолжает доминировать за счет более существенно низкой стоимости, а также возможности применения в качестве идентификатора смартфона пользователя с возможностью биометрической аутентификации. По оценке «М.Видео-Эльдорадо», 90 % биометрических смартфонов имеют дактилоскопический сканер отдельно или в сочетании с другими технологиями [3].

На Рисунке 2 представлены сферы, где оборудование и решение СКУД наиболее востребованы.

Создание программно-аппаратного комплекса СКУД является актуальной задачей. Согласно действующим трендам в области СКУД комплекс должен обеспечивать следующие функциональные особенности:

- обеспечение политики доступа пользователей к защищаемому объекту в зависимости от прав доступа;
- обеспечение учета событий посещения защищенного объекта;
- безопасная передача информации в сетях передачи данных;
- использование биометрических данных клиентов.

Проектирование программно-аппаратного комплекса

В качестве описания поведения системы разрабатываемого программно-аппаратного комплекса была применена диаграмма вариантов использования для выявления пользовательских и функциональных требований.

Рисунок 2. Сферы, где оборудование и решение СКУД наиболее востребованы

Диаграмма вариантов использования программно-аппаратного комплекса представлена на Рисунке 3.

Рисунок 3. Диаграмма вариантов использования программно-аппаратного комплекса

Согласно приведенному сценарию при помощи панели администратора осуществляется создание клиентов и точек входа-выхода (дверей), если ранее они были не созданы. Соз-

данные двери должны быть проинициализированы, то есть запущено программное обеспечение контроллера управления и пройдена процедура идентификации на сервере. После инициализации дверей для подтверждения подлинности контроллера управления должна быть пройдена процедура аутентификации. Доступ к двери осуществляется при помощи устройства пользователя, на котором формируется список возможных точек входа-выхода, которые пользователь может открыть. Аутентификация и авторизация пользователя происходит при помощи выданного ему логина и пароля. При каждом открытии двери добавляется новая запись о взаимодействии с контроллером управления в журнале событий.

Диаграмма последовательности описывает жизненный цикл объекта и взаимодействие действующих лиц информационной системы в рамках прецедента. На Рисунке 4 показана процедура инициализация точки входа-выхода с участием панели администратора, контроллера управления и сервера.

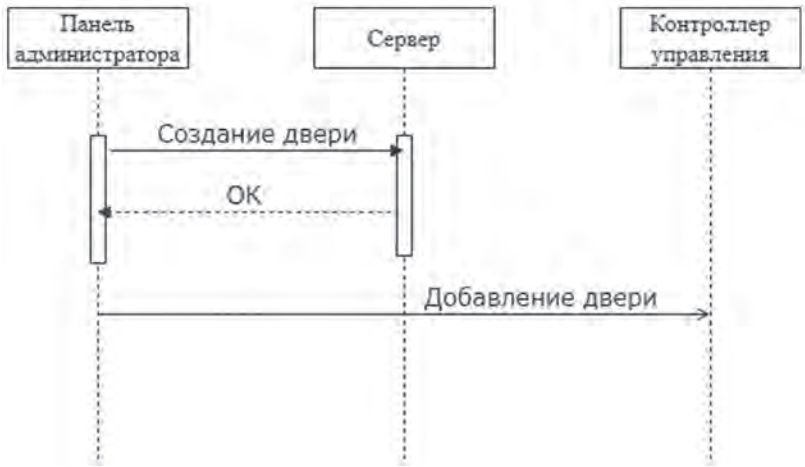

Рисунок 4. Инициализация точки входа-выхода

При инициализации точки входа-выхода генерируется пара ключей шифрования для использования ассиметричного алгоритма RSA. После генерации ключей шифрования при помощи панели управления на сервер отправляется HTTP-запрос на создание новой точки входа-выхода с указанием ее названия и публичного ключа, и в случае ответа от сервера «200 OK» новая дверь будет создана. Непосредственное добавление двери на контроллер управления осуществляется путем сохранения приватного ключа при помощи flash-карты и USB-разъема на контроллере.

На Рисунке 5 описана процедура авторизации точки входа-выхода с участием устройства пользователя, контроллера управления и сервера.

После отправки контроллеру управления сообщения о начале инициализации на сервер, сервер отправляет сообщение, в котором передаются случайное целое число и зашифрованный при помощи публичного ключа точки входа-выхода идентификатор сервера. Контроллер управления осуществляет расшифровку полученных данных своим приватным ключом и для подтверждения ключей шифрования отправляет расшифрованное целое число на сервер. После сравнения сервер подтверждает точку входа-выхода и переводит ее в состояние «подключена», после чего подтвержденная точка становится доступной для пользователей системы на устройстве пользователя, и сервер отправляет на

контроллер управления пару маркеров. Отправка маркеров происходит в зашифрованном виде по подтвержденным ранее ключам шифрования.

Рисунок 5. Аутентификация точки входа-выхода

На Рисунке 6 описана процедура взаимодействия устройства пользователя с точкой входа-выхода с участием устройства пользователя, контроллера управления и сервера. После поступления на устройство пользователя биометрического подтверждения и успешной проверки биометрических данных устройство пользователя отправляет запрос на контроллер управления для открытия двери с указанием маркера доступа и тем самым инициализирует соединение. Контроллер управления к полученному сообщению добавляет свой маркер аутентификации и передает полученное сообщение на сервер. Сервер на основании маркеров отправляет ключ открытия двери, зашифрованный публичным ключом контроллера управления, на устройство пользователя. Устройство пользователя отправляет подтверждение открытия точки входа-выхода посредствам этого ключа. Контроллер управления отправляет на сервер расшифрованный ключ открытия точки входа-выхода. На сервере производится процедура верификации полученного ключа, и в случае успеха на контроллер управления отправляется идентификатор, зашифрованный публичным ключом контроллера управления. Контроллер управления сравнивает полученный идентификатор с сохраненным значением и при совпадении осуществляет открытие двери. Также сервер отправляет сообщение пользователю на устройство пользователя об удачном открытии двери. После выполненных операций контроллер управления и устройство пользователя обновляют маркеры доступа, сервер осуществляет запись в журнал событий проведенного взаимодействия.

Проектирование схемы базы данных

База данных включает в себя описания содержания, структуры и ограничений целостности, используемых для создания и поддержки базы данных. База данных проектируемой СКУД включает в себя таблицы, описывающие пользователей (Users), точки входа-выхода (Doors), записи в журнале аудита (Audit). Каждая из сущностей содержит уникальный первичный ключ. Для построения связей «многие ко многим» используется дополнительная ассоциативная таблица (Association), содержащая записи первичных ключей связанных объектов.

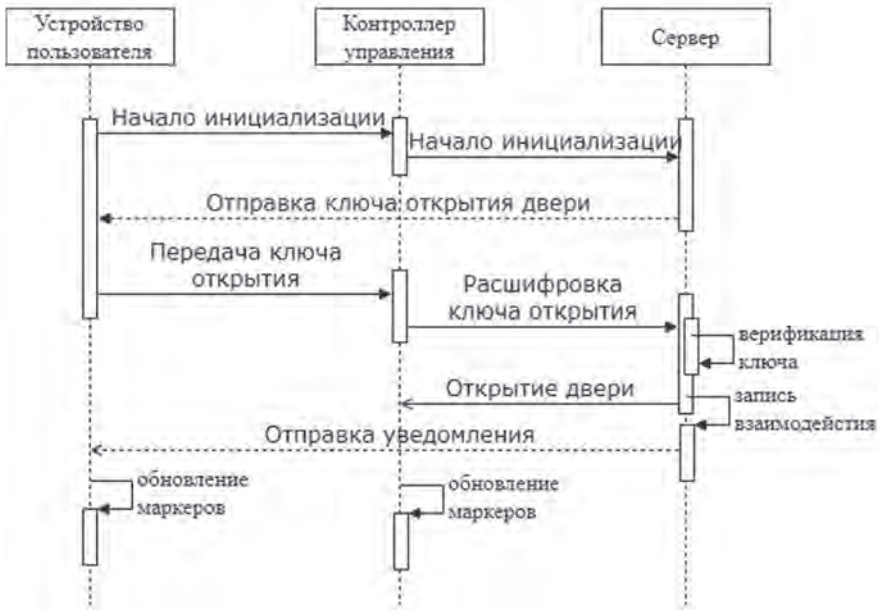

Рисунок 6. Взаимодействие пользователя с точкой входа-выхода

Программно-аппаратный комплекс поддерживает распределение ролей в системе «пользователь – администратор». Администратор имеет возможность инициировать точки входа-выхода, создавать пользователя, просматривать журнал аудита, изменять роль пользователя в системе. Пользователь имеет возможность взаимодействовать с точками входа-выхода посредством пары маркеров доступа, имеющих ограниченное и настраиваемое время жизни во временной шкале и в количестве выполняемых запросов. Пользователь имеет ссылки на список доступных дверей. Публичный ключ шифрования точки входа-выхода хранится на сервере в таблице Doors. Статус активности точки входа-выхода позволит определить доступность открытия точки входа-выхода с указанием пользователей, которым доступна дверь. Записи в таблице журнала Audit хранят информацию о двери, времени и пользователе, прошедшем через указанную дверь.

Схема базы данных приведена на Рисунке 7.

Заключение и выводы

Рассмотрены основные возможности СКУД, поставлены основные цели и задачи для разрабатываемого программно-аппаратного комплекса контроля доступа с использованием биометрической системы идентификации и аутентификации посредством мобильного устройства. Аппаратная часть СКУД реализована на микрокомпьютере Raspberry, для реализации программного обеспечения использовались языки программирования Python, Kotlin, Swift и JavaScript. При проектировании системы были построены: диаграмма вариантов использования, схема базы данных и диаграмма последовательности, описывающая процедуры инициализации и аутентификации точки входа-выхода, взаимодействия пользователя с точкой входа-выхода. Система обеспечивает гибкую интеграцию с корпоративными сервисами предприятия.

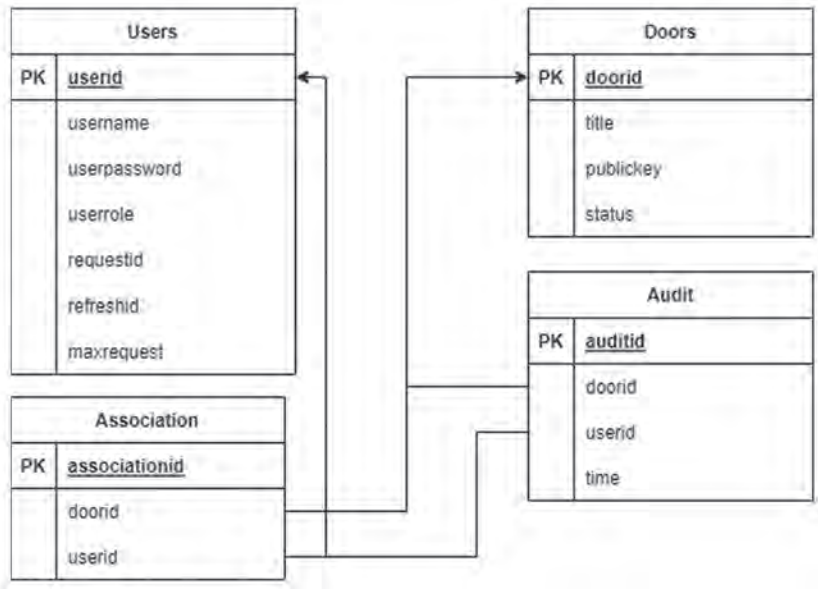

Рисунок 7. Схема базы данных

Литература

1. Аналитика мирового и российского рынка контроля доступа в прогнозах мировых агентств [Электронный ресурс]. URL: http://www.techportal.ru/security/access-control/rossiyskiy-i-mirovoy-rynki-skud-tsifry-prognozy-i-trendy/ (дата обращения: 18.03.2022).

2. Архитектура СКУД: прошлое, настоящее, будущее [Электронный ресурс]. URL: https://www.secuteck.ru/articles/arhitektura-skud-proshloe-nastoyashchee-budushchee (дата обращения: 18.03.2022).

3. Биометрическая идентификация (рынок России) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Биометрическая_ идентификация_(рынок_России) (дата обращения: 18.03.2022).

4. ГОСТ Р 54831–2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования: национальный стандарт Российской Федерации (введен 2012.09.01).

5. ГОСТ Р 51241–2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний: национальный стандарт Российской Федерации (введен 2009.09.01.).

6. Рынок контроля доступа достигнет 13,1 млрд долларов к 2026 году. [Электронный ресурс]. URL: https://www.secuteck.ru/news/rynok-kontrolya-dostupa-dostignet-13-1-mlrd-dollarov-k-2026-godu (дата обращения: 18.03.2022).

7. СКУД: современные подходы, требования и решения // Безопасность зданий и сооружений. 2020. № 1. С. 28–37.

8. Сравнительная характеристика СКУД. [Электронный ресурс]. URL: https://www.rgsec.ru/stati/sravnitelnaya-harakteristika-skud (дата обращения: 18.03.2022).

9. Широкий рынок – разная динамика [Электронный ресурс]. URL: http://lib.secuteck.ru/articles2/sys_ogr_dost/shirokiy-rynok-raznaya-dinamika (дата обращения: 18.03.2022).

References

1. *Analitika mirovogo i rossijskogo rynka kontrolya dostupa v prognozah mirovyh agentstv* [Analytics of the world and Russian market of access control in the forecasts of world agencies]. Available at: http://www.techportal.ru/security/access-control/rossiyskiy-i-mirovoy-rynki-skud-tsifry-prognozy-i-trendy/ (date of the application: 18.03.2022) (in Russian).

2. *Arhitektura SKUD: proshloe, nastoyashchee, budushchee* [ACS architecture: past, present, future]. Available at: https://www.secuteck.ru/articles/arhitektura-skud-proshloe-nastoyashchee-budushchee (date of the application: 18.03.2022) (in Russian).

3. *Biometricheskaya identifikaciya (rynok Rossii)* [Biometric identification (market of Russia)]. Available at: https://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(рынок_России) (date of the application: 18.03.2022) (in Russian).

4. GOST R 54831-2011. *Sistemy kontrolya i upravleniya dostupom. Ustrojstva pregrazhdayushchie upravlyaemye. Obshchie tekhnicheskie trebovaniya: nacional'nyj standart Rossijskoj Federacii (vveden 2012-09-01)* [GOST R 54831-2011. Access control and management systems. Controlled blocking devices. General technical requirements: national standard of the Russian Federation (introduction date 2012-09-01)] (in Russian).

5. GOST R 51241-2008. *Sredstva i sistemy kontrolya i upravleniya dostupom. Klassifikaciya. Obshchie tekhnicheskie trebovaniya. Metody ispytanij: nacional'nyjstandart Rossijskoj Federacii (vveden 2009-09-01)* [GOST R 51241-2008. Means and systems of control and management of access. Classification. General technical requirements. Test methods: national standard of the Russian Federation (introduction date 2009-09-01)] (in Russian).

6. *Rynok kontrolya dostupa dostignet 13,1 mlrd dollarov k 2026 godu* [The access control market will reach $13.1 billion by 2026]. Available at: https://www.secuteck.ru/news/rynok-kontrolya-dostupa-dostignet-13-1-mlrd-dollarov-k-2026-godu (date of the application: 18.03.2022) (in Russian).

7. *SKUD: sovremennye podhody, trebovaniya i resheniya* [ACS: modern approaches, requirements and solutions]. *Bezopasnost' zdanij i sooruzhenij*, 2020, No. 1, pp. 28–37 (in Russian).

8. *Sravnitel'naya harakteristika SKUD* [Comparative characteristics of ACS]. Available at: https://www.rgsec.ru/stati/sravnitelnaya-harakteristika-skud (date of the application: 18.03.2022) (in Russian).

9. *Shirokij rynok – raznaya dinamika* [Broad market – different dynamics]. Available at: http://lib.secuteck.ru/articles2/sys_ogr_dost/shirokiy-rynok-raznaya-dinamika (date of the application: 18.03.2022) (in Russian).