Научная статья
Original article
УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ПОСТРОЕНИЯ КОМБИНИРОВАННЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

ENSURING INFORMATION SECURITY BY BUILDING COMBINED ACCESS CONTROL AND MANAGEMENT SYSTEMS

Горохов Александр Владимирович, младший научный сотрудник, Военная академия связи им. С.М. Буденного, г. Санкт-Петербург, тел. 8(962) 410-42-95, sanya.gorokhov.97@mail.ru

Гаврин Виталий Алексеевич, младший научный сотрудник, Военная академия связи им. С.М. Буденного, г. Санкт-Петербург, тел. 8(996) 595-04-75, gavrin96@mail.ru

Мартынов Вячеслав Андреевич, младший научный сотрудник, Военная академия связи им. С.М. Буденного, г. Санкт-Петербург, тел. 8(911) 982-39-47, tesla.mva1996@gmail.com

Gorokhov Alexander Vladimirovich, junior researcher, Marshal Budyonny Military Signal Academy, Saint Petersburg, тел. 8(962) 410-42-95, sanya.gorokhov.97@mail.ru

Gavrin Vitaly Alekseevich, junior researcher, Marshal Budyonny Military Signal Academy, Saint Petersburg, тел. 8(996) 595-04-75, gavrin96@mail.ru

Martynov Vyacheslav Andreevich, junior researcher, Marshal Budyonny Military Signal Academy, Saint Petersburg, тел. 8(911) 982-39-47, tesla.mva1996@gmail.com

Аннотация. Представленная работа посвящена изучению инновационного подхода к обеспечению информационной безопасности, связанного с построением комбинированных систем контроля и управления доступом. Автором решается ряд задач, посредством которых доказывается гипотеза о том, что такие инструменты обеспечения информационной безопасности являются достаточно эффективными и качественными. Научная новизна заключается в методологическом изучении инновационного метода построения систем контроля и управления доступом.

Abstract. The presented work is devoted to the study of an innovative approach to information security related to the construction of combined access control and management systems. The author solves a number of problems by means of which the hypothesis is proved that such tools for ensuring information security are sufficiently effective and of high quality. The scientific novelty lies in the methodological study of the innovative method of building access control and management systems.

Ключевые слова: информационная безопасность, система контроля, управление доступом, комбинация, информация

Keywords: information security, control system, access control, combination, information

Проблема обеспечения информационной безопасности продолжает занимать ключевые места в секторе информационных технологий на сегодняшний день. В большей степени данный фактор является следствием повсеместной цифровизации современного общества, а также бытовых и профессиональных сфер жизнедеятельности человека. Именно недостаточный уровень обеспечения информационной безопасности способен привести к колоссальным потерям материального и экономического характера [1].

Другой причиной необходимости развития систем информационной безопасности и, в частности, систем контроля и управления доступом (СКУД) является совершенствование алгоритмов и махинаций киберпреступников. Повсеместная цифровизация общества порождает различные кибернетические атаки. Исходя из этого, с целью обеспечения должного уровня работы информационных систем на предприятиях необходимо повсеместное развитие и

повышение уровня обеспечения информационной безопасности в специализированных системах.

Таким образом, представленная работа преследует своей целью решение проблемы необходимости разработки интеграции инновационных комбинированных СКУД.

Системы контроля и управления доступом представляют из себя совокупность совместимых между собой средств аппаратного и программного уровня. Каждый из данных инструментов направлен с целью ограничения доступа людей, транспорта и иных объектов в те или иные помещения или территории. Именно посредством СКУД происходит предупреждение несанкционированного доступа к засекреченной, корпоративной или иной информации на объекте.

Системы контроля и управления доступом имеют достаточно примитивный вид, включая считыватель, приемник, сервер и другое. На рис. 1 представлен пример СКУД на предприятии, основанной на пропусках и турникетах.

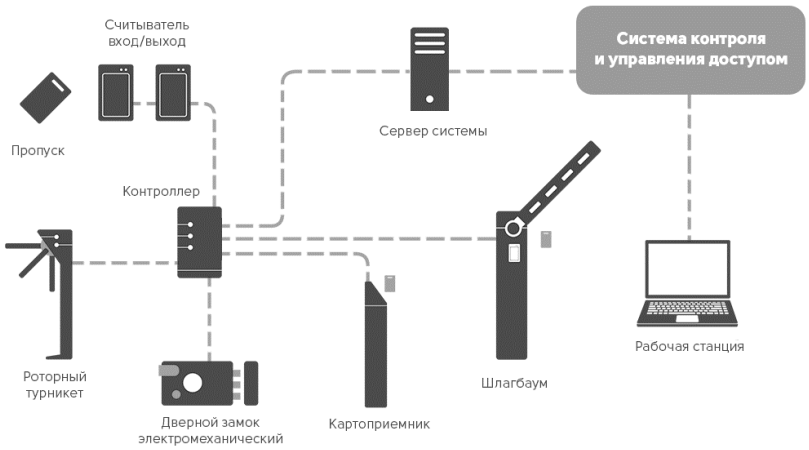

Рис. 1. Примитивная схема СКУД

Современные СКУД устаревают ввиду интенсивного распространения и улучшение алгоритмов работы хакерских атак на информационные системы предприятия. Таким образом, современные системы контроля и управления доступа необходимо незамедлительно развивать и совершенствовать, интегрируя инновационные алгоритмы и технологии [2].

Одним из наиболее актуальных и эффективных направлений инновационного развития СКУД является интеграция интеллектуальных технологий, в частности,

средств видеонаблюдения с целью автоматического выявления несанкционированного доступа. Это стало возможным благодаря развитию фотокамер и переход на цифровые аппараты, имеющие высокую четкость. Перспективные средства видеонаблюдения способны в автоматическом режиме детектировать движение в указанных областях кадра, а также выполнять многокамерное сопровождение объекта, измеряя статистические и биометрические признаки человека [3].

Другим перспективным решением для систем контроля и управления доступом является нанесение на документы RFID-идентификаторов. Активный радиочастотный идентификатор, представляющий собой наклейку, позволит отслеживать местонахождение предметов и документов в реальном времени. Также является перспективным использование активных RFID-пропусков для бесконтактной идентификации. Особенно преимущество этой технологии проявляется в аварийных ситуациях в условиях свободного прохода. Когда сохраняется возможность зарегистрировать всех лиц, покинувших охраняемую зону.

Необходимо подчеркнуть, что наиболее перспективным вариантом развития СКУД является разработка комбинированных систем, включающих в себя множество специализированных программ и функций и имеющий наибольшую эффективность в отказе от несанкционированного доступа (рис. 2) [4].

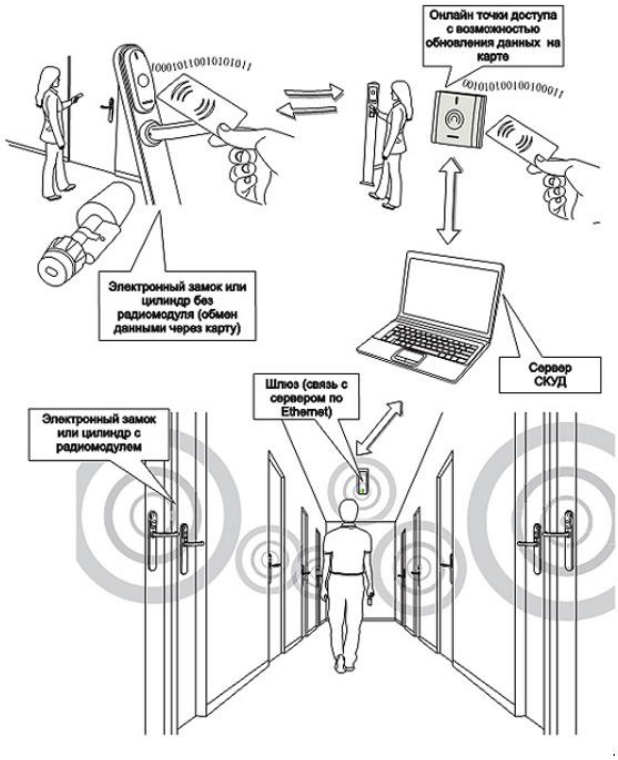

Рис. 2. Схема комбинированной СКУД

Разработчики и производители комбинированных средств аутентификации представляют на рынок инновационные решения, включающие биометрические карты. Основным преимуществом данной технологии является возможность не устанавливать биометрические считыватели, а использовать установленные считыватели смарт-карт. Таким образом, на биометрической карте находится сканер отпечатков пальцев с 3D-технологий и RFID-чип, посредством которого обеспечивается поддержка популярных технологий по стандарту ISO 14443. Такой способ обновления СКУД является весьма экономным способом перехода с устаревших технологий, использующих проксимити карты на биометрические технологии.

В комбинированных системах контроля и управления доступом карта является на только носителем данных о доступе пользователя, но и работать в роли флешки, посредством которой база данных СКУД и точки доступа обмениваются информацией в обоих направлениях. Для того чтобы этот обмен происходил максимально оперативно и комфортно производится комбинация различных типов точек доступа в одной системе.

Основное отличие онлайн-контроллеров СКУД комбинированной системы от «обычных» состоит в том, что они не просто работают в режиме реального времени, но также выполняют роль промежуточного портала в обмене данными между картой и БД СКУД. В момент прохода через такую точку доступа карта «соединяется» с БД СКУД и происходит описанный выше двухсторонний обмен данными [5].

Таким образом, основной целью данной статьи являлось изучение актуальности и перспективности использования комбинированных систем контроля и управления доступом для защиты информации на предприятии.

В заключение необходимо отметить, что цифровизация ставит перед современным общество огромное количество задач, связанных обеспечением информационной безопасности. Именно за счет должного уровня обеспечения информационной безопасности современные предприятия смогут ограничить материальные и экономические потери, а также рационализировать свою деятельность.

Литература

1. Голубкин Н.Д. Тенденции развития систем контроля и управления доступом в помещение // Вестник магистратуры. 2021.
2. Терехов К.Г. Направления совершенствования систем контроля и управления доступом для радиационно-опасных объектов // Глобальная ядерная безопасность. 2018.
3. Devitsyna S.N., Yeletskaya T.A., Balabanova T.N., Gakhova N.N. Development of an intelligent biometric user identification system // Economy. Computer science. 2019.
4. Марьенков А.Н., Кузнецова В.Ю., Гелагаев Т.М. Применение технологий распознавания лиц в системах контроля и управления доступом // Прикаспийский журнал: управление и высокие технологии. 2021.
5. Zudinov A.S. Introduction of biometrics into access control systems at critical information infrastructure facilities // StudNet. 2021.

References

1. Golubkin N.D. Trends in the development of systems for monitoring and managing access to the premises // Bulletin of the Magistracy. 2021.
2. Terekhov K.G. Directions for improving access control and management systems for radiation-hazardous objects // Global Nuclear Safety. 2018.
3. Devitsyna S.N., Yeletskaya T.A., Balabanova T.N., Gakhova N.N. Development of an intelligent biometric user identification system // Economy. computer science. 2019.
4. Mar'enkov A.N., Kuznetsova V.Yu., Gelagaev T.M. Application of face recognition technologies in access control systems // Caspian journal: management and high technologies. 2021.
5. Zudinov A.S. Introduction of biometrics into access control systems at critical information infrastructure facilities // StudNet. 2021.

© Горохов А.В., Гаврин В.А., Мартынов В.А., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №4/2022.

Для цитирования: Горохов А.В., Гаврин В.А., Мартынов В.А. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ПОСТРОЕНИЯ КОМБИНИРОВАННЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №4/2022.