РАЗДЕЛ II. МЕНЕДЖМЕНТ И УПРАВЛЕНИЕ ОРГАНИЗАЦИЕЙ

Абдулхаликова А.И.

Системы контроля и управления доступом в корпоративных информационных системах

Дагестанский государственный университет
(Россия, Махачкала)

doi:10.18411/sciencepublic-08-05-2020-06

idsp: sciencepublic-08-05-2020-06

Научный руководитель
Дадаева Б.Ш.

Аннотация

Система управления и контроля доступом. Обеспечение защиты информации в корпоративных информационных системах с помощью системы управления и контроля доступом. Основные части системы управления и контроля доступом.

Ключевые слова: система контроля и управления доступом, устройства преграждающие, устройства считывающие, идентификаторы, средства управления в составе аппаратных устройств и программных средств.

Abstract

Access control and management System. Ensuring information security in corporate information systems using access control and management systems. The main parts of the access control system.

Keywords: access control and control system, blocking devices, reading devices, identifiers, control tools as part of hardware devices and software.

Системы контроля и управления доступом (СКУД) в настоящее время получили довольно широкое распространение. СКУД используются для поддержания и обеспечения режима безопасности на предприятии, в том числе и для обеспечения защиты информации в корпоративных информационных системах.

Использование системы контроля и управления доступом позволяет не только контролировать доступ к защищенному объекту, но и сделать этот процесс более удобным и быстрым. А программное управление позволяет гибко настроить функционирование системы контроля и управления доступом. Например, доступ по расписанию, когда для каждого клиента задается расписание доступа к защищенному объекту, обеспечивается разграничение уровней доступа, контроль соблюдения режима работы и контроль за передвижением клиента[1].

Система контроля и управления доступом позволяет обеспечить защиту информации в корпоративных информационных системах при недобросовестной конкуренции в условиях современного бизнеса. В таких условиях для любого предприятия встает проблема обеспечения безопасности его основных активов. Системы контроля и управления доступом могут сыграть решающую роль при расследовании инцидентов, так как эти системы ведут журналы событий, в которые заносится информация обо всех взаимодействиях пользователя со СКУД.

Система контроля и управления доступом представляет собой совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью[3].

Разработка и постановка на производство средств и систем контроля управления доступом должны производиться в соответствии с ГОСТ Р 15.201. Средства СКУД

должны обеспечивать непрерывное функционирование и работу в автоматическом режиме, за исключением случаев чрезвычайных, аварийных и тревожных ситуаций, а также по требованию заказчика. Система контроля и управления доступом должна защищать объект от несанкционированного доступа, контролировать и вести учет посетителей охраняемого объекта. Кроме того, СКУД не должны создавать препятствий для доступа к объектам со свободным входом. Для непрерывного функционирования СКУД должны быть снабжены резервным источником питания, переход на который должен осуществляться в автоматическом режиме без нарушения установленных режимов работы и функционального состояния[1].

Основными частями СКУД являются:

1. Устройства преграждающие (управляемые);
2. Устройства считывающие;
3. Идентификаторы (ИД);
4. Средства управления в составе аппаратных устройств и программных средств.

В состав СКУД могут входить другие дополнительные средства: источники электропитания; датчики (извещатели); дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления устройствами; устройства преобразования интерфейсов сетей связи; аппаратуру передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД. В состав СКУД могут входить также аппаратно-программные средства и средства вычислительной техники (СВТ) общего назначения.

В ходе изучения СКУД решаются следующие задачи:

1. Получение студентами базовых теоретических сведений по функционированию биометрических систем, систем на основе RFID-карт, ключей iButton, домофонов, usb-ключей eToken.
2. Знакомство с реальным оборудованием СКУД на специализированном стенде и обучение его администрированию.
3. Исследование погрешностей аутентификации пользователей СКУД [2].

Заключение

Внедрение корпоративной информационной системы дает организации следующие преимущества:

- возможность принимать обоснованные решения;
- улучшение качества обслуживания клиентов;
- улучшение взаимоотношений с поставщиками;
- возможность повышения производительности труда.

Однако, чтобы достигнуть повышения эффективности деятельности организации, к выбору информационной системы необходимо подходить очень серьезно.

Выбор корпоративной информационной системы для внедрения является достаточно сложным процессом, который требует тщательного анализа как текущих потребностей и финансовых возможностей организации, так и перспективных планов его развития. Наилучший эффект от внедрения корпоративной информационной системы достигается при ее комплексном развертывании и максимальной заинтересованности руководства предприятия в успехе всего проекта.

1. ГОСТ Р 51241-2008. СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ. Классификация. Общие технические требования. Методы испытаний.
2. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. / Ворона В. А., Тихонов В. А. – М. : Горячая линия – Телеком, 2010. – 272 с.: ил.
3. Волхонский В.В. Системы контроля и управления доступом. / Волхонский В.В. – СПб: Университет ИТМО, 2015. – 200 с