

УДК 004.78:004.056.53

ОБЗОР ВИДОВ СИСТЕМ КОНТРОЛЯ ДОСТУПА НА ПРЕДПРИЯТИИ

Филитова Анастасия Александровна

магистрант

miss.filitova@mail.ru

Куденко Вячеслав Борисович

кандидат технических наук, доцент

melkud@ya.ru

Мичуринский государственный аграрный университет,

г. Мичуринск, Россия

Аннотация: представлена классификация современных систем контроля и управления доступом, представлены составляющие СКУД. Выявлена необходимость использования надежного ПО системы контроля и доступа.

Ключевые слова: системы контроля и доступа, контроллер, программное обеспечение, идентификатор.

В современном мире безопасности на объектах различной направленности уделяется особое внимание, вне зависимости от того, это крупное предприятие или небольшой офис, школа или торговый центр. Наряду с традиционным штатом сотрудников охраны, занимающихся выполнением этих функций, используются различные технические системы, расширяющие возможности и функциональность служб охраны.

Система контроля и управления доступом, или СКУД – это элемент системы безопасности, созданный на основе технических устройств и электронных систем управления, объединённых в единую сеть, работающую на специально разработанном программном обеспечении [1, 2].

Системы контроля доступа различаются по способу управления ими и подразделяются на два основных вида – автономные и сетевые.

Автономные системы не предполагают централизованного управления с использованием компьютерной техники. Их легче монтировать, они не требуют прокладки протяженных кабельных линий, дешевы, просты в эксплуатации и достаточно эффективны [2, 3]. Существенный недостаток автономных систем в том, что они не умеют накапливать и хранить информацию, а следовательно, вести учет рабочего времени, перемещений персонала и формировать отчеты. Кроме того, отсутствие централизованного управления затрудняет, а на крупных объектах с множеством точек доступа и с разным уровнем секретности подразделений – делает невозможным своевременное удаление и занесение кодов идентификаторов [1, 4].



Рисунок 1 – Схема подключения автономной СКУД

Сетевые системы контроля и управления доступом управляются центральным компьютером, что позволяет оперативно и одновременно менять ключи доступа для всех преграждающих устройств (проходных, дверей, ворот). Память и программное обеспечение компьютера, соединенного со всеми точками контроля перемещений, накапливают и систематизируют информацию о прошедших (проехавших) на объект, позволяют вести учет рабочего времени и контролировать трудовую дисциплину сотрудников. Сетевые системы контроля наиболее совершенны, многофункциональны и незаменимы при организации управления доступом на крупных предприятиях со сложной структурой, обширной территорией и многочисленным персоналом. Кроме того, посредством компьютерного управления сетевые комплексы могут быть интегрированы в единую систему безопасности объекта наряду с системой видеонаблюдения, охранно-пожарной сигнализацией и прочими [4, 5].



Рисунок 2 – Схема подключения сетевой СКУД

Универсальные СКУД включают в себя функции как автономных, так и сетевых систем. Работают в сетевом режиме под управлением центрального устройства и переходят в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или при обрыве связи [4, 6, 7].

Определившись с типом СКУД, придется выбрать еще и комплект необходимого оборудования. Рынок предлагает великое множество устройств, разнообразных по функционалу, надежности и цене. Независимо от вида системы (сетевая или автономная), набор оборудования будет состоять из

контроллеров, считывателей, идентификаторов, а также заграждающих устройств различного типа.



Рисунок 3 – Схема подключения биометрической (по отпечатку пальца) СКУД

Контроллер – это, по сути, администратор доступа: именно он определяет, кого и куда следует пропускать. Контроллер «помнит» все введенные оператором идентификаторы и права каждого из них. В сетевых системах контроллером является центральный компьютер. В автономных системах контроллеры – электронные приборы, рассчитанные на обслуживание одной точки доступа или нескольких [1, 3, 8].

Считыватели – это устройства, которые способны прочесть код идентификатора и передать его контроллеру для принятия решения. Сложность и конструкционные особенности считывателя определяются типом идентификаторов, для которых они предназначены. Основным критерий эффективности и функциональности считывателя – быстрота идентификации и передачи данных [9, 10].

Идентификаторы – это ключи-носители кода, который и определяет права доступа их владельца в те или иные объекты. Идентификаторы могут быть механическими, магнитными, оптическими, электронными, радиочастотными. Наиболее часто используются контактные электронные ключи и бесконтактные, в виде карточек или брелоков. доступа. Бесконтактные ключи на сегодня – самый оптимальный вариант по сочетанию надежности и цены [5, 10, 11]

Заграждающие устройства – это великое множество разновидностей электромеханических замков и защелок для дверей, турникеты, шлагбаумы, электроприводные ворота, болларды, шлюзовые кабины. Их выбор определяется соображениями целесообразности и удобства эксплуатации.

Серьезную, если не основную роль в успешном функционировании СКУДов играет используемое программное обеспечение. Программные модули обеспечивают построение всей распределенной системы контроля, организуют взаимодействие различных устройств и передачу данных между ними. Кроме того, в многофункциональных сетевых системах используется программное обеспечение, отвечающее за ведение баз данных, учет количественных характеристик и формирование отчетов, а также за дополнительные функции видеоверификации в режиме реального времени и интеграцию с прочими компьютерными управляющими системами.

Приобретая систему по управлению доступом, необходимо понимать, что СКУД – сложная система из множества различных компонентов, монтаж и внедрение которой можно доверить только квалифицированному персоналу солидных компаний [3, 11, 12]. Специалисты помогут также определиться с выбором технических и программных средств, профессионально проанализировав особенности объекта заказчика и его возможности. При этом важен не только грамотный выбор и монтаж системы, но и последующее гарантийное и постгарантийное техническое обслуживание, которое заключается, прежде всего, в периодической диагностике средств контроля. Своевременное сервисное обслуживание – гарантия стабильной работы системы, а значит, и снижения рисков, связанных с несанкционированным доступом на подконтрольный объект.

Список литературы:

1. ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. - Введ. 01.01.2015.

2. Приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20. Порядок проведения классификации информационных систем персональных данных.
3. РД 78.36.005-99. Выбор и применение систем контроля и управления доступом.
4. РД 78.36.003-2002. Руководящий документ Инженерно-техническая укрепленность. Технические системы охраны. Требования и нормативы проектирования по защите объектов от преступных посягательств.
5. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2017. - 272 е.: ил.
6. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом. - М.: Экополис и культура, 2017.
7. Подготовка инженерных кадров в области техносферной безопасности в разрезе аграрного университета / И.П. Криволапов, С.Ю. Щербаков, К.А. Манаенков [и др.]// В сб: Техносферная безопасность как комплексная научная и образовательная проблема. – Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», 2018. – С. 177-181
8. Характеристика методов проведения анализа риска / С.Ю. Щербаков, И.П. Криволапов, Д.И. Стрельников [и др.] // Наука и Образование. – 2019. – Т. 2. – № 4. – С. 253.
9. Совершенствование физической защиты объектов хранения и распределения нефтепродуктов в сельском хозяйстве / С.Ю. Щербаков, И.П. Криволапов, А.А. Заборских [и др.] // Наука и Образование. – 2019. – Т. 2. – № 2. – С. 232.
10. Коротков, А.А. Современные технические устройства по защите от ионизирующего излучения на производстве / А.А. Коротков, И.П. Криволапов // В сб.: Инженерное обеспечение инновационных технологий в АПК: материалы

Международной научно-практической конференции. – Мичуринск: Мичуринский государственный аграрный университет, 2018. – С. 51-54.

11. Васильков, А.С. Модернизация системы цифрового видеонаблюдения инженерного института Мичуринского ГАУ / А.С. Васильков, В.Б. Куденко // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 37.

12. Филитова, А.А. Этапы проектирования систем контроля и управления доступом ООО «ГРАНИТ-М» / А.А. Филитова, В.Б. Куденко // Наука и Образование. – 2020. – Т. 3. – № 2. – С. 38.

UDC 004.78:004.056.53

OVERVIEW OF TYPES OF ACCESS CONTROL SYSTEMS IN THE ENTERPRISE

Filitova Anastasia Alexandrovna

master's degree

miss.filitova@mail.ru

Kudenko Vyacheslav Borisovich

Candidate of Technical Sciences, Associate Professor

melkud@ya.ru

Michurinsk state agrarian University

Michurinsk, Russia

Annotation. The classification of modern control and access control systems is presented, the components of the ACS are presented. The necessity of using reliable software of the control and access system is revealed.

Key words: control and access systems, controller, software, identifier.