СОВРЕМЕННЫЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

М.Л. Сагидова, *канд. техн. наук, доцент*
Филиал Мурманского арктического государственного университета в г. Апатиты (Россия, г. Апатиты)

DOI:10.24412/2500-1000-2022-9-1-64-68

Аннотация. *Обеспечение должного уровня защиты и безопасности являются важными вопросами в рабочей деятельности любой современной организации. В рамках данного исследования был осуществлено рассмотрение современных систем контроля и управления доступом. Системы данного рода являются одним из современных инструментов, применяемого для решения вопросов обеспечения безопасности – они позволяют ограничить доступ к помещениям организации, контролировать передвижения сотрудников. Применение систем данного рода, еще и в совокупности с видеонаблюдением и сигнализацией предоставляют организации существенное количество преимуществ. В статье приводится описание функционала современных СКУД, их типовой состав и варианты реализации, а также основные отечественные производители и их системы. В зависимости от требований касаемо охраны помещений или помещений организации, системы контроля и управления доступом могут иметь различный охват и состоять как из пары устройств, так и из целого комплекса оборудования, что трактуется потребностями организации, а также имеющимся бюджетом.*

Ключевые слова: *СКУД, контроль и управления доступом, системы управления и контроля доступом, обеспечение безопасности.*

Краткое описание системы контроля и управления доступом может быть представлено как совокупность аппаратно-технического обеспечения, объединенного посредством сети передачи данных, целью функционирования которых является:

- защита территории и помещений организации от проникновения, а имущества от порчи или хищения;
- осуществление контроля и учета прибытия и убытия персонала на рабочие места, а также въезда и выезда транспортных средств;
- идентификация лиц, которым разрешен доступ на охраняемую территорию [1].

В первую очередь СКУД внедряют с целью обеспечения защиты организации, однако системы данного рода реализуют и ряд дополнительных возможностей:

- выполнение учета рабочего времени персонала организации;
- интеграция с бухгалтерскими системами для автоматизированного расчета заработной платы;
- интеграция с пожарной и охранной сигнализацией для построение единого охранного периметра;
- формирование базы данных и ведение журнала учета посетителей в организации.

В том случае, когда СКУД объединяют с видеонаблюдения в организации имеется возможность совместить друг с другом возникновение определённых событий, например в случае открытия двери без ключа доступа система сделает запись в журнал событий, сохранит запись события в файл и в журнале сделает пометку с наименованием данного файла [2].

Принцип работы любой системы контроля и управления доступом основан на считывании специального идентификатора посредством устройства-считывателя и управления специальными устройствами – калиткой, турникетом, дверью, воротами и т.д. Если карта будет успешно считана, то дверь откроется, а турникет будет разблокирован, и сотрудник сможет пройти далее. В противном случае ничего не произойдет. И в обоих случаях будет выполнена запись о возникновении события – как положительного считывания ключ-

карты и пропуска её владельца, так и о попытке проникнуть в охраняемое помещение или на территорию с неактивной или ошибочной ключ-картой.

В зависимости от требуемого уровня обеспечения защиты помещений предприятия реализуемая СКУД может иметь разный уровень сложности касаемо её архитектуры [3].

Для современных систем контроля и управления доступом может быть выполнена классификация на основании нескольких различных критериев. Так, в зависимости от метода управления системой СКУД классифицируют как следующие виды:

- автономные СКУД, представляющие собой самостоятельные устройства, размещаемые, как правило, в одной точке прохода. Это объединение считывателя и запорного механизма в одном корпусе, данные системы обладают ограниченной памятью на количество хранимых идентификаторов и чаще всего не имеют функционала по ведению журнала возникающих событий. Применяются для защиты отдельных помещений, или входа в здание.

- сетевые СКУД являются классической системой контроля и управления доступом. Они предназначены для организации комплексной защиты – содержат в своем составе целый набор различных считывателей и электромагнитных замков, объединенных сетевыми подключениями с серверной платформой, на которую установлено специальное программное обеспечение, управляющее системой и предоставляющее возможность взаимодействия со СКУД оператору;

- биометрические СКУД являются наиболее современными и технологичными, однако они не особо распространены по причине их высокой стоимости.

В зависимости от используемого ключевого идентификатора системы контроля и управления доступом классифицируются как:

- бесконтактные, в которых используются Proxmity-карты, либо карты с нанесенным на них штрих-кодом. Данный вариант организации считывателей в СКУД можно назвать более удобным для пользователей, по той причине, что при их использовании карты не прикладываются к считывателям;

- контактные – это СКУД, в которых в качества ключа доступа используются магнитные карты, либо так называемые «таблетки» в формате touch-memory брелока со встроенным в них чипом запоминающего устройства.

Также существует отдельная классификация СКУД, согласно которой их подразделяют на несколько классов:

1. Класс I – Сюда относятся простейшие системы, в состав которых как правило, входит обычный электронный замок с запирающим устройством. Системы данного класса обладают минимальным функционалом, а процесс идентификации сотрудников они могут сопровождать звуковыми, либо световыми сигналами.

2. Класс II – к данному классу относятся уже одноуровневые, либо многоуровневые СКУД, в которых права посетителей могут быть настроены как на основании выданных им идентификаторов, так и на основании различных временных рамок. Данные системы могут функционировать как автономно, так и посредством локальной вычислительной сети. В большинстве случаев система функционирует по сети, а в автономный режим переходит автоматически при потере связи либо при отключении электропитания.

3. Классы III и IV – сюда относят высококлассные сетевые СКУД, которые помимо контроля и управления доступом реализуют функционал по учету рабочего времени, интегрируются с системами видеонаблюдения и охранно-пожарной сигнализации, используют сложные идентификаторы, а также обладают многоуровневым взаимодействием [4].

На текущий момент на рынке СКУД в России можно выделить следующие готовые программно-аппаратные решения:

1. APACS 3000.
2. Lyrix.
3. Gate.
4. PERCo.
5. ИСО «Орион».
6. Parsec.
7. SIGUR.

8. IronLogic.
9. Smartec.
10. RusGuard.

Конечный выбор системы как по классу, так и по производителю в большинстве случае зависит от потребностей и требований к системе. Так, для домашнего использования возможно использование простейшей автономной системы, для среднего офиса подойдут системы второго класса, а вот в случае крупной организации потребуются уже более продвинутые решения, интегрируемые в общую систему обеспечения безопасности.

Говоря о системах контроля и управления доступом уже неоднократно отмечался тот факт, что это зачастую сложная система, в состав которой входят различные устройства [5]. К их числу относятся:

1. Контроллер – это центральное устройство, отвечающее за функционирование всей системы и входящей в её состав устройств. Непосредственно в нем хранятся все идентификаторы, на основании которых контроллером будет принято решение о допуске владельца идентификатора на охраняемую территорию. В том случае, если СКУД обладает довольно обширным масштабом, допускается использование в ее составе сразу нескольких контроллеров, которые объединяются между собой посредством сети передачи данных.

2. Исполнительные устройства в составе СКУД – это оборудование, управляемое контроллером. Устройства данного типа делят на две категории – устройства, монтируемые на дверях, и устройства, монтируемые на проходах. Данные устройства являются механизмами, которые более всего подвержены износу в рамках работы СКУД, по причине чего требуют выполнения не только настройки их работы, но и периодического технического обслуживания. К данным устройствам относятся:

- замки – монтируются на дверях. В СКУД чаще всего применяют электромагнитные и электромеханические замки. Для первых характерно наличие механизма автоматического открытия, по причине чего их чаще всего устанавливают на эвакуационных выходах. А вот электромеханические замки обладают защитой от перенапряжения или отключения напряжения, что делает их более устойчивыми ко взлому;

- защелки – электрические устройства, которые монтируются в дверях внутренних помещений. В отличие от замков обладают более низким уровнем защиты от взлома, и чаще всего могут быть открыты простым отключением электропитания;

- ворота – преграждающее устройство, которое устанавливается на входе на охраняемую территорию. Чаще всего комплектуется считывателем;

- турникет – устанавливается на входе в здание, либо непосредственно внутри здания в каком-то определенном проходе. Назначение данного устройства не столько в ограничении доступа, сколько для контроля прохода сотрудников и посетителей на охраняемую территорию;

- шлюзовые кабины – это специальные преграждающие устройства, которые чаще всего используются в организациях, в которых к безопасности предъявляются строгие требования;

- барьеры – это преграждающие устройства, которые размещают на въезде на контролируемую территорию. Используются для ограничения и контроля доступа на охраняемую территорию транспортных средств.

3. Идентификаторы – это устройства, в которых записывают специальный код доступа. Визуально представляют собой брелок, карту памяти или иной небольшой предмет, который выдается сотруднику, для которого был назначен записанный в идентификатор код доступа. Существует еще вариант, когда в роли идентификатора выступает специальный цифровой код, набираемые на цифровой панели доступа, либо в качестве идентификатора могут выступать определенные биометрические данные – отпечаток пальца, изображение сетчатки глаза и т.д.

4. Считыватели – устройства, выполняющие работу по считыванию кода из идентификатора и передаче его на контроллер. В зависимости от используемых в системе идентификаторов могут быть использованы и различные считыватели – начиная от простых считывателей магнит-

ных карт и заканчивая сканерами сетчатки глаза или отпечатка пальца.

5. Вспомогательное оборудование – это технические средства, которые применяют для обеспечения корректного взаимодействия между перечисленными выше элементами СКУД. Наиболее ярким примером данного оборудования являются конверторы сигналов, блоки питания, датчики и т.д. Их использование обусловлено необходимостью обеспечения надежной и удобной работы СКУД.

6. Программное обеспечение – это необязательный компонент СКУД, однако оно существенно расширяет функционал СКУД в плане контроля работы оборудования системы, выполнения анализа состояния устройств и оповещения ответственных сотрудников о различных происшествиях [6].

В завершении необходимо отметить, что распространение систем контроля и управления доступом происходит довольно активно. Эти системы используются не только в офисах, но и в жилых комплексах, по той причине, что они являются дополнительным и достаточно надежным рубежом защиты от проникновения на территорию нежелательных лиц. А в совокупности с другими системами позволяет реализовать достаточно функциональную систему защиты и обеспечения безопасности.

Библиографический список

1. Баранова, Е.К. Информационная безопасность и защита информации: учеб. пособие / Е.К. Баранова, А.В. Бабаш. – 3-е изд., перераб. и доп. – М.: РИОР: ИНФРА-М, 2017. – 322 с.

2. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2017. – 256 с.

3. Скрипник Д.А. Общие вопросы технической защиты информации. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 424 с. – [Электронный ресурс]. – Режим доступа: http://www.iprbookshop.ru/52161.html.

4. Внуков, А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования. – 3-е изд., перераб. и доп. – М.: Изд-во Юрайт, 2022. – 161 с.

5. Щеглов, А.Ю. Защита информации: основы теории: учебник для вузов / А.Ю. Щеглов, К.А. Щеглов. – М.: Изд-во Юрайт, 2021. – 309 с.

6. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О.В. Казарин, А.С. Забабурин. – М.: Изд-во Юрайт, 2021. – 312 с.

MODERN ACCESS CONTROL AND MANAGEMENT SYSTEMS

M.L. Sagidova, *Candidate of Technical Sciences, Associate Professor*
Branch of the Murmansk Arctic State University in Apatity
(Russia, Apatity)

Abstract. *Ensuring the proper level of protection and security are important issues in the work of any modern organization. Within the framework of this study, a review of modern access control and management systems was carried out. Systems of this kind are one of the modern tools used to solve security issues - they allow you to restrict access to the premises of the organization, control the movement of employees. The use of systems of this kind, also in conjunction with video surveillance and alarm systems, provide organizations with a significant number of advantages. The article provides a description of the functionality of modern access control systems, their typical composition and implementation options, as well as the main domestic manufacturers and their systems. Depending on the requirements regarding the protection of the premises or premises of the organization, access control and management systems can have different coverage and consist of both a pair of devices and a whole range of equipment, which is interpreted by the needs of the organization, as well as the available budget.*

Keywords: *ACS, access control and management, access control and management systems, security.*