

Применение систем контроля и управления доступом в инженерных сооружениях

Антоневич А.И.¹, Гуминский П.А.²

¹Белорусский национальный технический университет

²ОАО «Беллифт»

СКУД (система контроля и управления доступом) – это совокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещения определённого объекта.

С помощью системы идентификации (карта, брелок, отпечатки, универсальный код и т.д.), программа индивидуально для каждого рассчитывает его график работы, время прихода и ухода, время, потраченное на перерывы и обед.

Главными задачами систем контроля являются:

- наложение ограничений на вход;
- допуск в помещение определённому кругу лиц;
- контроль рабочего дня;
- обеспечение безопасности;
- расчет зарплаты, при интеграции с бухгалтерской системой.

Системы контроля и управления доступом имеют следующие составляющие:

- преграждающее устройство (электромагнитные замки, двери, турникеты);
- идентификатор (карточка, брелок, отпечаток пальца);
- контроллер – механизм, определяющий пропускную возможность идентификатора;
- считыватель – устройство, определяющее код идентификатора и передающее его на контроллер.

Можно выделять три группы систем:

Автономные системы. Такие устройства являются альтернативой дверным замкам, как правило, в коммерческих помещениях. В систему вносятся коды карт доступа, которым разрешён вход. При совпадении карты и запрограммированного кода в системе, замок

отпирается. Эти системы не требуют подключения к компьютеру и обладают минимальным набором функций.

Недостатки Автономной СКУД:

- В простых контроллерах доступа как правило нет возможности удалить отдельный ключ из памяти; чтобы удалить потерянные ключи, необходимо стереть всю память и заполнить заново актуальными.
- Простые автономные контроллеры не поддерживают расписания и группы доступа.
- Контроллер автономной СКУД не хранит информацию о входах и выходах пользователей.
- В отличие от сетевых и части биометрических СКУД автономные системы не предназначены для учета рабочего времени.

Сетевые. Такие СКУД имеют больше возможностей: они могут настраивать доступ в помещение по расписанию, контролируют график работы и интегрируются с видеокамерами, охранной и противопожарной системами. Сетевые системы соединены с компьютером и управляются дистанционно.

Недостатки Сетевой СКУД:

- Возможность взлома системы. Карты доступа могут быть потеряны или украдены, ими может воспользоваться злоумышленник, в отличие от биометрических систем, например, дактилоскопических, где существует защита от предъявления муляжей.

Биометрические системы. Эти системы контроля и управления доступом имеют индивидуальную направленность: уникальный код каждого сотрудника. В программу заносятся отпечатки пальцев или рисунок радужки глаза. Такой подход обеспечивает более высокий уровень безопасности и предоставляет более полную информацию по каждому сотруднику каждого отдела. С помощью биометрической системы есть возможность вести журнал посещений, контролировать время, потраченное работником на перерывы и командировки.

Достоинства Биометрической СКУД:

- Сотрудникам различных подразделений могут задаваться разные расписания и зоны доступа.

- Биометрическая система контроля доступа включает в себя функцию учета рабочего времени сотрудников и формирования отчетов по формам бухгалтерского учета.
- Сетевой контроллер доступа хранит журнал событий: входов, выходов пользователей и аварийных открытий двери.
- Проверка личности пользователя занимает всего несколько секунд.
- Биометрические показатели невозможно подделать.

Недостатки Биометрической СКУД:

- Биометрические системы контроля доступа дороже аналогичных систем, использующих для доступа бесконтактные карты. Но с каждым годом цена становится ниже.
- При числе пользователей более 1000 необходимо введение двухфакторной системы идентификации: по карте доступа и отпечатку.
- Временные пропуски невозможны.

Идентификаторы.

В качестве идентификатора может выступать - физический предмет, на который с помощью разных технологий заносится кодовая информация. В качестве носителя идентификационных данных может выступать как идентификаторы, специально созданные для этого, так и использоваться уже существующие, например, телефонный номер или банковская карта. Также в качестве идентификаторов могут выступать биометрические признаки человека. Наиболее часто в биометрических системах контроля доступа используются - отпечаток пальца, венозный рисунок пальца или руки, геометрия (форма) лица, радужная оболочка глаза.

Бесконтактные RFID идентификаторы

Наибольшее распространение получили идентификаторы передача данных, которых, основана на технологии бесконтактной передачи данных RFID. А самыми распространенными форм факторами будет соответственно пластиковая карта и брелок, хотя есть, конечно, еще и браслеты и целый гигантский ассортимент меток.

Считыватели предназначены для считывания и передачи кодовой информации с идентификатора в контроллер СКУД.

- Считыватели бесконтактных карт
- Считыватели банковских карт
- GSM считыватели для считывания телефонных номеров

- Считыватели контактных ключей Touch Memory
- Считыватели с кодонаборной панелью для введения пин кода

Препраждающие устройства:

-Турникеты.

Уникальной особенностью турникетов, которой лишены все прочие препраждающие устройства является отсечение проходящих по одному. Что делает их практически незаменимыми, когда стоит цель идентифицировать каждого входящего в здание человека.

- Турникеты триподы
- Турникеты с распашными створками
- Турникеты с раздвижными створками
- Полноростовые
- Полуросстовые роторные
- **Ворота для проезда транспорта;**
- **Болларды (дорожные блокираторы);**
- **Шлагбаумы;**
- **Шлюзовые кабины**

Шлюзовая кабина автоматическое устройство надежного контроля посетителей, представляющее собой автоматический тамбур-шлюз (шлюз безопасности). Кабина в пуленепробиваемом и взрывозащищенном исполнении (прямоугольной или цилиндрической формы) содержит два контура дверей, открывающихся и закрывающихся автоматически. Сквозной проход через шлюзовую кабину невозможен: в один момент времени может быть открыта только одна дверь, либо внутренняя, либо внешняя.

Контроллеры СКУД:

Автономные контроллеры СКУД

Автономные контроллеры как можно понять из их названия работают исключительно в автономном режиме, то есть к ним нельзя подключить другие контроллеры.

Сетевые контроллеры СКУД

Сетевые контроллеры сколько бы их не было с легкостью объединяются в одну сеть, и как правило подключаются к компьютеру с установленным программным обеспечением с которого легко и просто можно управлять всей системой доступа

Персональные компьютеры и программное обеспечение

Системное программное обеспечение для СКУД может иметь разные масштабы — от простого изолированного решения, устанавли-

ваемого на один ПК в незащищенной зоне до мощного сетевого пакета, установленного на сервер, находящийся в охраняемом помещении с контролируемым доступом.

Литература

1. Британская Ассоциация индустрии безопасности Руководство по составлению спецификаций на СКУД (перевод)/ Британская Ассоциация индустрии безопасности // 2021. 170 стр.

2. Владимир Рыкунов . Охранные системы и технические средства физической защиты объектов / Владимир Рыкунов .Security Focus, 2019. 284 с.