ПРОГРАММНОЕ СРЕДСТВО АВТОМАТИЗАЦИИ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ТЕРРИТОРИЮ ПРЕДПРИЯТИЯ

Петровский О.И., студент

Белорусский государственный университет информатики и радиоэлектроники,
Институт информационных технологий,
г. Минск, Республика Беларусь

Бакунов А.М. – ст. препод. каф. ИСИТ

В данной работе кратко рассмотрена система автоматизации и контроля управления доступом, их устройств и конфигурацию

Безопасность важна для любого бизнеса, будь то небольшой офис или крупный промышленный объект. Система контроля и управления доступом (СКУД) — одна из основных систем контроля, которую современные компании используют, чтобы следить за тем, кто, когда и зачем посещает территорию предприятия. Использование подобных систем, наряду с традиционным штатом сотрудников службы охраны, дает бизнесу немало преимуществ.

СКУД – это набор объединенных в единую сеть аппаратно-технических средств, которые позволяют решить ключевые задачи безопасности:

- предотвратить проникновение на частную территорию посторонних лиц;
- организовать учет рабочего времени, фиксацию времени въезда и выезда транспортных средств;
- защитить материальные ценности, включая производственное и офисное оборудование, от повреждений и кражи.

Базовые элементы любой СКУД — идентификатор, считыватель, исполнительное устройство и контроллер (подробно о каждом из них можно прочитать в конце статьи). Для работы подобных систем используется специализированное программное обеспечение, которое настраивается индивидуально, исходя из сложности системы и конкретных целей установки.

Вне зависимости от конфигурации, в любой системе такого рода есть 4 основных компонента:

1. Контроллер. Это устройство — «мозг» системы. Именно контроллер хранит информацию обо всех сотрудниках, посетителях и правах доступа, которые есть у каждого из них. Программирование сетевых СКУД осуществляется через компьютер. В автономных системах вместо этого используются отдельные электронные приборы, позволяющие управлять одной или несколькими точками доступа.
2. Идентификаторы. Представляют собой ключи с уникальным кодом.

По карточке пропускная система на предприятии определяет, в какие помещения и зоны может войти владелец.

3. Считыватели. Устанавливаются непосредственно на точках доступа – возле дверей, ворот и так далее. Могут быть контактными или бесконтактными. Ключевые критерии эффективности считывателя — скорость идентификации и передачи данных. Оптимальная высота установки считывателей СКУД – 120 см от пола.

4.Заграждающие устройства. В зависимости от того, как работает система СКУД, это могут быть турникеты, электроприводные ворота, электромеханические дверные замки. Перед помещениями, где хранятся деньги, дорогостоящее оборудование, опасные вещества и другие ценности, часто устанавливаются блокирующие шлюзовые кабины.

Принцип работы СКУД прост: пользователь подносит идентификатор к считывателю. Тот получает код и передает информацию на контроллер, который принимает решение о предоставлении доступа. Если проход разрешен, система посылает сигнал на запирающее устройство, и дверь открывается.

Сложность и конфигурация системы контроля доступа в офис зависят от требований к безопасности. Современные СКУД можно классифицировать по нескольким критериям:

1. По способу управления:

1. Сетевые. В качестве контроллера используется сервер — компьютер, на котором установлено соответствующее программное обеспечение. Сетевые СКУД легко интегрировать с системами видеонаблюдения, пожарной сигнализации. Функционал позволяет не только организовать контроль доступа, но и вести учет рабочего времени, следить за состоянием дверей, добавлять и изменять пользователей, карты-доступа, шаблоны доступа и так далее.
2. Автономные. Самостоятельное оборудование, рассчитанное на 1-2 точки прохода. Считывающий прибор и электромагнитный замок находятся в одном корпусе. Обычно используются для защиты офисов и других небольших объектов, поскольку максимальное количество пользователей ограничено.

3. Биометрические. Самый прогрессивный тип СКУД. Используются крайне редко: для обычных предприятий установка подобного оборудования слишком затратна и не оправдана.

1. По типу идентификатора:

1. Бесконтактные. Используют Proxmity-карты или карты со штрих- кодом. Считаются более удобными, поскольку для разблокировки запирающего механизма их не нужно прикладывать к считывателю
2. Контактные. Могут работать на магнитных картах.

2. По классу:

1. I класс. Простейшие системы управления доступом с автоматическим запирающим устройством. Имеют минимум необходимых функций и работают автономно. Идентификация пользователей может сопровождаться звуковыми и световыми сигналами.
1. II класс. Одно- или многоуровневые монофункциональные сети, позволяющие настроить права доступа посетителей как по идентификатору, так и по времени и дате. Большинство таких систем поддерживают возможность работы как в автономном режиме, так и по сети.
2. III и IV классы. Высококлассные сетевые СКУД с учетом рабочего времени, большим количеством функций, сложными идентификаторами и многоуровневым взаимодействием.

Список использованных источников:

1. Ворона, В. А. Системы контроля и управления доступом : справочное издание В. А. Ворона, В. А Тихонов. – Москва: Горячая линия – Телеком, 2010. – 272 с.

2. Кормен Т. Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест. – М.: МЦНМО, 2009. – 960 с.