Использование смарт-карт в системе контроля и управления доступом (СКУД)

Грибова Василина Вячеславовна
Студент, факультет информатики и математики,
Амурский государственный университет
г. Благовещенск, РФ
E-mail: gvasilin@mail.ru

Система контроля и управления доступом (СКУД) — это обязательный элемент комплексной системы безопасности и неотъемлемая часть современного офиса, как система электронного документооборота или система кондиционирования. В работе рассматриваться использование смарт-карт в данной системе.

Картами доступа или магнитными картами, обычно, называют электронный ключ, заключенный в пластиковую или картонную карту. Смарт-карта (*ICC* — карта с интегрированными электронными цепями), способный принять запрос от считывателя и ответить на него своим уникальным кодом — идентификатором. Устройств с подобным принципом работы сейчас огромное количество, Смарт-карты находят применение в различных областях, от систем накопительных скидок до кредитных, дебетовых карт, студенческих билетов, телефонов стандарта GSM, проездных билетов и многое другое.

Основной принцип работы смарт-карты — получить запрос, а в ответ сообщить свой уникальный код, который не повторяется, его сложно подделать и перехватить удаленно. При построении любой Системы Контроля и Управления Доступом (СКУД, СКД), построенной на базе карт и ключей доступа, именно на этот код и смотрит система для идентификации. То есть такие системы не смотрят на лица, паспортные данные, пол и возраст пользователей, они видят только код, полученный в ответ на запрос, и если этот код занесен в базу главного устройства (контроллера) — система разрешит доступ. Так работают самые простые СКУД — Автономные. Разработанная система построена на более сложных устройствах, с применением сервера, к данному уникальному коду добавлена дополнительная информация — ФИО, фото, секция, комната, номер общежития. На самих же картах так и остается — только код. Сделано это, в первую очередь, для сохранности данных, ведь в противном случае, при потере рабочую карты доступа, злоумышленник мог бы узнать данные. Во вторую очередь, это делается для того, чтобы система работала как можно быстрее. Сообщить устройству считывания, даже самый длинный код — дело нескольких долей секунды, а вот скачать с карты фото, довольно сложная задача, и в-третьих, это значительно удешевляет систему в целом и каждый отдельный ключ в частности. В разработанной системе смарт-карта используется в качестве пропуска, полностью заменяя бумажный эквивалент. При предъявлении карты подаётся специальный сигнал, в случае если пропуск активен, то сигнал одного типа, если пропуск окончил своё действие либо вовсе отсутствует в базе, то сигнал подаётся другой. Плюс к сигналу если пропуск недействителен, то вместо фотографии будет выведено изображение с соответствующей надписью. За время эксплуатации системы, было выявлено «тонкое» место системы, а именно — считыватель ACR122U, в результате чего было принято решение о необходимости разработки и внедрение считывателя отвечающим всем требованиям стабильности работы. Таким образам новый считыватель стал базироваться на микроконтроллере AT328-P. Считыватели ACR122U были выведены из эксплуатации не полностью, они продолжили функционировать, в качестве настольных считывателей, при присвоение уникального индикатора жильцам. 21

Так же переход на программируемый микроконтроллер позволит в бедующем отказаться от персональных компьютеров на пунктах охраны, путем выполнения основных обработок непосредственно на считывателе, который в свою очередь будет выводить информацию о проходах на любое мобильное устройство под управлением Android или Windows, что заметно сократит затраты при интеграции системы и повысит ее отказоустойчивость, а так же позволит подключать периферийные устройства вида турникет, калитка или любую другую преграждающую конструкцию.

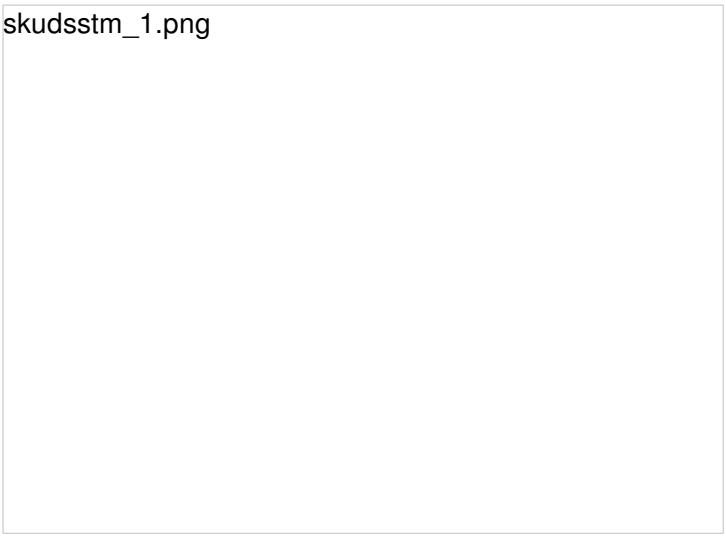

Рисунок 1 — Считыватель смарт карт

Список литературы

1. Антимонов С. Г., Сердюк В. А. Мониторинг событий информационной безопасности и защита персональных данных // ДиалогНаука. 2013 г. — С 24
2. Журков Д.А. Защита персональных данных от утечки по техническим каналам// ДиалогНаука. 2013 г. — С 14
3. Клаус Финкенцеллер. Справочник по RFID. Теоретические основы и практическое применение индуктивных радиоустройств, транспондеров и бесконтактных чип-карт // Додэка. 2008 г. — С 496