УДК 681. 5. 017

Разработка СКУД с максимальной отказоустойчивостью и методы обеспечения ее бесперебойной работы

Густова Джесика Ренартовна

Магистрант 2 курса, кафедра И9 БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова,

г. Санкт-Петербург

E-mail: jesika1995@yandex.ru

Системы контроля управления доступом (СКУД) прочно заняли свое место в перечне технических систем безопасности, предлагаемых на рынке. Вместе с охранно-пожарной сигнализацией и системами телевизионного наблюдения, они образуют базу для интеграции систем безопасности зданий в единый комплекс.

СКУД позволяет обеспечить в любое время контроль над ситуацией, порядок, безопасность персонала и посетителей. Кроме того, СКУД дает возможность контролировать трудовую дисциплину, производить учет использования персоналом своего рабочего времени и многое другое.

СКУД – совокупность аппаратных, программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта.

Таким образом, центральным элементном СКУД является контроллер – устройство, предназначенное для обработки информации, поступающей от считывателей, идентификаторов, для принятия решения и управления исполнительными устройствами.

Важнейшим аспектом в работе СКУД является гарантированность защищенности информации, территории, имущества, а также безопасности жизнедеятельности.

Для контроля и организации максимально эффективного рабочего процесса, необходимо автоматизировать часть процессов, задачами которых являются службы безопасности, отдел охраны труда, а так такие вопросы, как учет рабочего времени, контроль охраняемой территории и прочее.

Следовательно, требуется произвести анализ организационную структуры службы безопасности.

Для того, чтобы гарантировать требования, предъявляемые к службам безопасности, к разрабатываемой СКУД предъявляются следующие требования:

-Высокие показатели отказоустойчивости.

- Защищенность от взломов.

- Возможность самотестирования на предмет неисправностей.

- Способность резервного восстановления основных элементов управления.

Сравнивая различные существующие системы, были выявлены уязвимости, которые следует отнести к критическим недостаткам СКУД:

1. Рассматривая охранные сигнализации, существенной угрозой работоспособности системы является наличие большого количества устройств постановки радиочастотной помехи для нарушения взаимодействия и обмена информацией элементов сигнализации, а также для подавления каналов связи и реагирования в случае появления тревожного сигнала.

Для устранения данного недостатка необходимо разработать проводной канал с функцией проверки работоспособности ключевых элементов системы.

2. На примере нескольких автономных СКУД, выявилось некорректное расположение центральной системы управления, а также отсутствие резервных тревожных систем, которые бы позволяли выявлять и сигнализировать о неполадках в центральной системе управления.

Одной из важных задач СКУД является корректная, безошибочная идентификации пользователя. Как правило, доступ разграничивается с помощью персональных RFID меток, ключей формата Touch Memory, QR-кодов, либо биометрических данных (отпечатки пальцев, сканирование радужной оболочки глаза, сетчатки, распознавание лиц).

Выполнив анализ методов авторизации пользователя и рассмотрев возможность двухфакторной аутентификации, был выявлена один из наиболее распространенных методов идентификации пользователя в СКУД – RFID (Radio Frequency IDentification).

Были рассмотрены типы атак, применяемые в технологии RFID. Из чего было определенно, что метод идентификации RFID содержит в себе достаточное количество уязвимостей и не удовлетворяет требованиям разрабатываемой системы.

Понимая, что проблема идентификации личности, при допуске к закрытой информации или объекту, всегда была ключевой, следует изучить современные биометрические системы.

Биометрические системы обеспечивают контроль доступа в следующих сферах:

- Передача и получение конфиденциальной информации личного или коммерческого характера.

- Регистрация и вход на электронное рабочее место.

- Осуществление удаленных банковских операций.

- Защита баз данных и любой конфиденциальной информации на электронных носителях.

- Пропускные системы в помещения с ограниченным доступом.

Биометрические характеристики являются очень удобным способом аутентификации человека, так как обладают высокой степенью защиты и их невозможно украсть, забыть или потерять.

Дактилоскопия (распознавание отпечатков пальцев) – наиболее разработанный на сегодняшний день биометрический метод идентификации личности.

К преимуществам метода следует отнести: высокую достоверность – статистические показатели метода лучше показателей способов идентификации по лицу, голосу, росписи; низкую стоимость устройств, сканирующих изображение отпечатка пальца; простая процедура сканирования отпечатка.

Недостатком метода является возможность повреждения папиллярного узора отпечатка пальца (мелкие царапины, порезы), что может привести к невозможности идентификации личности пользователя.

Оценив все возможные варианты биометрической идентификации личности, было решено в разрабатываемой системе использовать дактилоскопический метод идентификации пользователя.