

Балтийский государственный технический университет  
«ВОЕНМЕХ» им. Д. Ф. Устинова

## **Отчет по научно – исследовательской работе в семестре**

Тема магистерской диссертации:

**«Разработка системы контроля управления доступом (СКУД) с максимальной отказоустойчивостью и методы обеспечения ее бесперебойной работы»**

Выполнила: Густова Д. Р.

Группа: И9М31

Руководитель: Готин С. В.

Санкт-Петербург

2018 г.

## Содержание

Введение.....	3
1. Разработка алгоритмов взаимодействия и идентификации элементов СКУД.....	4
Заключение.....	8
Список использованных источников.....	9

## Введение

Системы контроля и 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.

Любая СКУД предназначена для того, чтобы автоматически пропускать тех, кому это положено, и не пропускать тех, кому это запрещено, контролируя тем самым перемещения сотрудников и посетителей на территории предприятия.

СКУД позволяет в любое время обеспечить 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.

Контроллерная СКУД – это 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. При их действительном многообразии все они работают по единой схеме: оборудование (запорно-пропускной механизм, будь то турникет, шлагбаум, проходная кабина и любое другое управляемое преграждающее устройство, а также считыватели - устройство, предназначенное для считывания (ввода) идентификационных признаков и др.) подключается к контроллеру, который в свою очередь подсоединяется к компьютеру.

Таким образом, центральным элементом данного класса СКУД является контроллер — устройство, предназначенное для обработки информации, поступающей от считывателей, идентификаторов, для принятия решения и управления исполнительными устройствами. Поэтому его часто называют «сердцем СКУД».

Поскольку тематикой магистерской диссертации была выбрана: «Разработка системы контроля управления доступом (СКУД) с максимальной отказоустойчивостью и методы обеспечения ее бесперебойной работы», первым этапом было выполнить следующие задачи:

- Разработать алгоритмы взаимодействия и идентификации элементов СКУД.
- Подобрать элементную базу.



# 1 Разработка алгоритмов взаимодействия и идентификации элементов СКУД

Важнейшим аспектом в работе системы контроля управления доступом (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 также такие вопросы, как учет рабочего времени, контроль охраняемой территории и прочее.

Следовательно, первостепенной задачей является анализ организационную структуры службы безопасности.

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) за рубежом определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации, деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью. В зарубежных источниках, например, рассматривается следующая структура службы безопасности фирмы. Она возглавляется начальником службы безопасности, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

С учетом накопленного зарубежного и отечественного опыта и особенностей рыночной экономики предлагается рабочий вариант службы безопасности предприятия среднего масштаба производства, ее структура и должностные инструкции.



- 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.

Уровень угрозы безопасности со стороны террористов и криминальных элементов привел к широкому использованию биометрических систем защиты и управления контролем доступа не только в государственных организациях или больших корпорациях, но и у частных лиц. В быту наиболее широко такое оборудование применяется в системах доступа и технологиях управления типа «умный дом».



Рисунок 2 – Биометрические средства идентификации.



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

Дактилоскопия (распознавание отпечатков пальцев) — наиболее разработанный на сегодняшний день биометрический метод идентификации личности. Катализатором развития метода послужило его широкое использование в криминалистике 20 века.

Каждый человек имеет уникальный папиллярный узор отпечатков пальцев, благодаря чему и возможна идентификация. Обычно алгоритмы используют характерные точки на отпечатках пальцев: окончание линии узора, разветвлении линии, одиночные точки. Дополнительно привлекается информация о морфологической структуре отпечатка пальца: относительное положение замкнутых линий папиллярного узора, «арочных» и спиральных линий.

Особенности папиллярного узора преобразовываются в уникальный код, который сохраняет информативность изображения отпечатка. И именно «коды отпечатков пальцев» хранятся в базе данных, используемой для поиска и сравнения. Время перевода изображения отпечатка пальца в код и его идентификация обычно не превышает 1 секунды, в зависимости от размера базы. Время, затраченное на поднесение руки — не учитывается.

### **Преимущества и недостатки метода**

***Преимущества метода.*** Высокая достоверность — статистические показатели метода лучше показателей способов идентификации по лицу, голосу, росписи. Низкая стоимость устройств, сканирующих изображение отпечатка пальца. Достаточно простая процедура сканирования отпечатка.

***Недостатки метода.*** Папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами. Люди, использовавшие сканеры на предприятиях с численностью персонала порядка нескольких сотен человек заявляют о высокой степени отказа сканирования. Многие из сканеров неадекватно относятся к сухой коже и не пропускают стариков. Так же присутствует недостаточная защищённость от подделки изображения

отпечатка, отчасти вызванная широким распространением метода. Для некоторых людей с «неподходящими» пальцами (особенности температуры тела, влажности) вероятность отказа в доступе может достигать 100%. Количество таких людей варьируется от долей процентов для дорогих сканеров до десяти процентов для недорогих. Конечно, стоит отметить, что большое количество недостатков вызвано широкой распространённостью системы, но эти недостатки имеют место быть и проявляются они очень часто.

Исходя из выше изложенного, в разрабатываемой системе контроля управления доступом будет использоваться дактилоскопия для идентификации пользователя.

## **Заключение**

В результате курсовой работы была выполнена задача разработки алгоритма взаимодействия и идентификации элементов СКУД.

Были изучены технологии RFID, их особенности и недостатки.

Были рассмотрены системы идентификации и аутентификации. Подробно рассмотрены средства биометрической идентификации.

Для разрабатываемой СКУД был выбран метод дактилоскопической идентификации пользователя, который будет являться основным.



### Список использованных источников

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2001.
2. Барсуков В.С. Интегральная защита информации // Системы безопасности. – М., 2002.
3. Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.
4. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.
5. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия - Телеком, 2000.
6. Сабынин В.Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост радиоэлектроники и телекоммуникации, 2001.