Государственное бюджетное профессиональное образовательное учреждение

«Южно-Уральский Государственный технический колледж»

**ИССЛЕДОВАНИЕ РЫНКА СИСТЕМ КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ И РАЗРАБОТКА МАКЕТА АВТОНОМНОЙ СКУД**

**Техническое направление**

***Исследовательский проект с реализацией действующего макета и фрагмента демонстрационного видеофильма***

Авторы (творческий коллектив):

Бусыгин С, Ладонкин А., студент

Руководители проекта:

Михайленко Ю.Н.,преподаватель

Стариков В.В., преподаватель

Челябинск

2020

**АННОТАЦИЯ**

Проект на тему: «Исследование рынка систем контроля управления доступом и разработка автономной СКУД" предусматривает анализ рынка СКУД и разработку макета системы, используемой для регистрации прохождения людей на объект.

В проекте представлены конструктивные элементы состава систем контроля доступа, проанализированы и сравнены способы идентификации, типы исполнительных механизмов СКУД, обоснован выбор типа системы контроля и управления доступом.

Конкретизированы положительные и отрицательные стороны технологий систем контроля доступа, проведен анализ потенциала рынка систем контроля и управления доступом (СКУД) Челябинской области.

Практическая реализация системы контроля и управления доступом представлена в виде макета варианта автономной СКУД на базе контроллера LC-1DW, который предназначен для изучения СКУД, а также получение навыков программирования и работы с СКУД во всех режимах, также разработан демонстрационный фильм по использованию макета на практических работах в учебном заведении.



**ОГЛАВЛЕНИЕ**

|  |  |
| --- | --- |
| Введение | 3 |
| 1 Теоретическое обоснование исследуемой области  1.1 Состав систем контроля управления доступом (СКУД)  1.2 Анализ и выбор способа идентификации  1.3 Анализ и выбор исполнительных механизмов СКУД  1.4 Принципы работы систем контроля управления доступом  1.5 Классификация и обоснование выбора способа управления СКУД  2 Практическое обоснование исследуемой области  2.1 Исследование рынка систем контроля и управления доступом  2.2 Моделирование архитектуры макета системы  2.3 Программирование системы  Заключение  Список используемой литературы | 6  6  7  12  14  16  18  18  23  32  40  44 |

**ВВЕДЕНИЕ**

Осуществление безопасности, контроль доступа являются одними из самых важных и значительных проблем на многих объектах Российской Федерации в наше время. Системы безопасности привлекают к себе достаточно большое внимание, многочисленные работы посвящены этой проблеме.

Поэтому **тема** - исследование рынка систем контроля управления доступом (СКУД) с разработкой автономной СКУД, позволяющей осуществить контроль доступа на объект.

Традиционные методы персональной идентификации, основанные на применении паролей или материальных носителей, таких как пропуск, паспорт, водительское удостоверение, не всегда отвечают современным требованиям безопасности. Решением проблемы является использование системы контроля и управления доступом (СКУД). Эти системы предназначены для обеспечения санкционированного прохода в помещения и охраняемые зоны.

Российский рынок систем безопасности - относительно молодой рынок. Основные факторы развития рынка - положительный финансовый климат России, рост культуры использования систем безопасности, рост рисков угроз и рост доли систем безопасности российского производства. По оценкам специалистов, системы контроля и управления доступом являются наиболее перспективными, одни из лидирующих, наравне с рынками систем охранной сигнализации и систем наблюдения.

Но ситуация складывается так, что рынок СКУД в настоящее время достаточно большой, как иностранного, так и российского производства, динамика роста не известна. В таких условиях оптимальный выбор конкретной модели СКУД весьма проблематичен. Тем более при реализации конкретных СКУД используют различные способы и реализующие их устройства для идентификации и аутентификации личности, разнообразие которых предстоит исследовать.

Комплексное применение систем позволит решить возникающие проблемы безопасности, ведь хорошо организованная с использованием современных технических средств СКУД позволит решать целый ряд задач. К числу наиболее важным можно отнести следующие:

- противодействие промышленному шпионажу, воровству, умышленному повреждению материальных ценностей;

- учет рабочего времени;

- контроль своевременности прихода и ухода сотрудников;

- регулирование потока посетителей;

- контроль въезда и выезда транспорта.

**Цель исследования** - анализ рынка и самих технических средств систем СКУД, разработка архитектуры макета автономной СКУД на базе контроллера LC-1DW, его практическая реализация. Под архитектурой здесь понимается организационная структура системы (макета), включающая в себя устройства, механизмы взаимодействия и основные принципы работы систем СКУД.

**Объектом исследования** являются системы безопасности.

**Предмет исследования** является перспективный сегмент рынка систем безопасности - системы контроля и управления доступом.  
Для достижения поставленной цели необходимо решить следующие **задачи**:

- изучить состав СКУД, на основе изученных материалов произвести сравнение и анализ систем;

- проанализировать и выбрать способ идентификации, исполнительные механизмы СКУД;

- рассмотреть принципы работы, сравнить способы управления системой;

- разработать материалы для исследования рынка СКУД;

- провести аналитическое исследование, обработать результаты, обобщить и представить результаты;

- смоделировать архитектуру макета автономной СКУД на базе контроллера LC-1DW;

- изготовить макет, наглядно демонстрирующий принцип работы СКУД

и протестировать макет, подтверждающий возможность использования.

Для достижения целей мы применили методы анализа, сравнения, обобщения, моделирования, программирования, метод опроса и опытно- поисковой работы. Характер работы действующий макет.

В рамках поставленных задач предполагается разработка автономной системы контроля и управления доступом, назначение данной СКУД обеспечить автоматическую фильтрацию посетителей по признаку - можно войти/нельзя, которая позволит контролировать ситуацию, безопасность персонала, сохранность материальных ценностей и информации, а также порядок на объекте. Данная система достаточно наглядная, макет, который будет понятен любому пользователю.

Таким образом, выбранная тема проекта «Исследование рынка систем контроля доступа с разработкой автономной СКУД» является актуальной, отражающей запросы общества.

Практическая ценность заключается в разработке действующего макета.

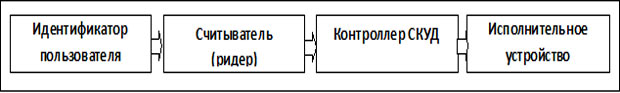
Разработанный проект рекомендован для использования в учебном процессе при закрепления теоретических знаний по теме «Системы контроля и управления доступом», в получении практических навыков, программировании контроллера, изучении режимов работ контроллера. Предназначен для студентов и специалистов, а также в качестве выставочного образца в профориентационной работе учебного учреждения.

**1 ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ИССЛЕДУЕМОЙ ОБЛАСТИ**

**1.1 Состав систем контроля управления доступом (СКУД)**

СКУД – это совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, территорий.

Структурная схема СКУД приведена на рисунке 1.

Рисунок 1 - Структурная схема СКУД

В общем виде СКУД может иметь в своем составе следующие элементы:

а) исполнительные механизмы (замки, турникеты, шлюзы);

б) электронные идентификаторы (пластиковые карточки, «электронные таблетки» и другие устройства);

в) считыватели (пластиковых карточек и прочих электронных идентификаторов);

г) устройства ввода персонального кода (PIN-кода);

д) биометрические устройства идентификации личности;

е) устройства управления исполнительными механизмами (контроллеры, концентраторы);

ж) оборудование сопряжения локальной сети СКУД с компьютером;

з) программное обеспечение администратора системы.

Система контроля и управления доступом обычно состоит из серверов– обычных компьютеров, которые управляют подключенными к ним контроллерами СКУД.

**Контроллер** (контрольная панель) – это основная часть системы управления доступом, в нем хранится информация о конфигурации, режимах работы системы, список людей, которые имеют право доступа к ресурсу, а также их привилегии доступа к этому ресурсу. Контроллер может быть встроен в считыватель, турникет, или другое исполнительное устройство.

**Считыватель** представляет собой устройство, которое позволяет считывать информацию, записанную на карточке и др. Эту информацию он передает контроллеру, который и принимает решение о допуске человека к ресурсу.

Любой считыватель предполагает ответную часть – **ключ-идентификатор**, который содержит информацию, с помощью которой происходит идентификация человека. Для повышения надежности идентификации кроме считывателей к контроллеру может подключаться клавиатура для набора персонального идентификационного номера (Пин-кода).

**1.2 Анализ и выбор способа идентификации СКУД**

Существует два различных направления в способах идентификации. Это идентификация с использованием электронных карт и использующая биометрические параметры человека.

Сейчас применяются следующие типы карт, каждому из которых соответствует определенный тип считывателя:

а) **магнитные карты** – считываются, при проведении в определенном направлении и с определенной скоростью по щели считывателя. Современные магнитные полосы изготовлены из материалов, требующих сильных магнитных полей для записи информации и, соответственно, для ее уничтожения, поэтому можно не бояться случайного размагничивания. Однако магнитные карты достаточно чувствительны к внешним воздействиям другого рода – загрязнению, влаге, царапинам. Еще один недостаток связан с необходимостью точного позиционирования в считывателе. Средний срок службы магнитных карт составляет около года, затем магнитный слой стирается. Поэтому магнитные карточки применяют, как правило, в системах, где предусмотрена частая замена карт, например, в отелях или на автостоянках;

б) **бесконтактные радиочастотные (PROXIMITY)** перспективный на сегодняшний день тип карт. Проксимити-считыватель постоянно посылает радиосигнал. Карта при попадании в зону действия считывателя принимает его излучение и в ответ посылает сигнал, содержащий записанный на микросхеме код. Расстояние между считывателем и картой зависит от мощности считывателя и варьируется от 5 см до нескольких метров. Отсутствие механического контакта в процессе работы позволяет делать идентификаторы произвольной формы (даже в виде гвоздя), идентификатор можно имплантировать в объект идентификации. Достоинствами являются сложность подделки, возможность применения криптоалгоритмов (шифрования).При этом карточка может находиться в кармане;

 в) **карты Виганда** – названные по имени ученого, открывшего сплав, обладающий прямоугольной петлей гистерезиса. Внутри карты размещены отрезки проволоки из этого сплава приклеенных специальным клеем, которые при перемещении мимо считывающей головки позволяют считать информацию. Эти карты более долговечны, чем магнитные, но и более дорогие. Один из недостатков – то, что код в карту занесен при изготовлении раз и  навсегда;

г) **штрих-кодовые карты** – на карту наносится штриховой код, кодовая информация записывается на магнитной полосе и содержится в изменяющейся ширине штрихов и расстоянии между ними. Код с такой карточки считывается оптическим считывателем. Штриховой код можно просто запачкать грязью. Магнитную карту легко поцарапать в кармане;

д) **Touch-memory** – металлическая таблетка, внутри которой расположен чип ПЗУ. При касании таблетки считывателя, из памяти таблетки в контроллер пересылается уникальный код идентификатора. Достоинствами являются компактность, высокая стойкость к механическим повреждениям, коррозии, перепадам температур и небольшая стоимость. Небольшой размер позволяет прикреплять контактную память практически на любом носителе — изделии, карточке, брелоке.

Биометрические системы идентификации наиболее эффективны, так как в них распознаются не физические носители информации, а признаки или особенности самого человека (уникальная персональная информация). Системы доступа и защиты информации, основанные на таких технологиях, являются не только самыми надежными, но и самыми удобными для пользователей на сегодняшний день. Все биометрические устройства предъявляют специфические требования к программным и аппаратным средствам.

К биометрическим способам идентификации относят:

а) **сканирование отпечатков пальцев** –является самым удобным методом. Преимуществом является и надежность сканирования отпечатков пальцев: несанкционированный доступ возможен примерно в одном случае из миллиона, а отказ в доступе уполномоченному пользователю возникает примерно в  3% случаев и связан в основном с неправильным уходом за сканером.

Существуют два основополагающих алгоритма распознавания отпечатков: по отдельным деталям (характерным точкам) и по рельефу всей поверхности пальца, а также комбинация этих алгоритмов. В дактилоскопических СКУД применяются алгоритмические решения, позволяющие отличить «живой» палец от «мертвого», – это определение температуры прикладываемого пальца, отслеживание во времени динамики потоотделения поверхности кожи пальца и характера деформации рисунка папиллярных линий на окне сканера.

б) **геометрия ладони и кисти рук** – технология идентификации человека по форме кисти руки основана на анализе трехмерного изображения кисти. Данный способ не является высоконадежным, что связано, в первую очередь с большой изменяемостью формы кисти как в течение жизни человека, так и в относительно короткие сроки;

в) **сканирование глаза** – различают два типа: сканирование радужной оболочки и  сканирование сетчатки. Устройство сканирования фактически представляет собой высококачественную телекамеру. Образец пятен на радужной оболочке находится на поверхности глаза. Видеоизображение глаза может быть отсканировано на расстоянии около метра. Такие устройства пока еще очень дороги. Сканирование сетчатки глаза происходит с использованием инфракрасного луча низкой интенсивности, направленного через зрачок к кровеносным сосудам на задней стенке глаза. В этом случае изображение радужной оболочки должно быть четким на задней части глаза, поэтому катаракта может отрицательно сказаться на качестве изображения радужной оболочки. С возрастом расположение пятен на радужной оболочке может меняться, причем довольно сильно. Ошибка негативной идентификации может возникнуть при самой небольшой травме глаза, вследствие бессонницы или повышенных нагрузок на глаза;

г) **идентификация по голосу** – чаще всего идентификация по характеристике голоса  осуществляется произнесением парольной фразы. Это удобный способ, но не такой надежный, как другие биометрические методы. Основная трудность заключается в большом разнообразии проявлений голоса одного человека – он может меняться в зависимости от настроения, состояния здоровья, возраста и многого другого. Еще одной серьезной проблемой в практическом применении идентификации личности по голосу является учет шумового компонента;

д) **подпись** – человек расписывается на специальном устройстве типа графического планшета. Компьютер сравнивает полученную написанную информацию с той, которая хранится в его базе, и в зависимости от результатов сравнения предоставляет доступ или отказывает в нем. Саму подпись легко подделать, но современные считыватели измеряют еще и характеристики движения руки при письме, что повышает надежность метода;

е) **геометрия лица**– этот метод слабо разработан. Лицевая термография – идентификация личности по схеме расположения кровеносных сосудов лица (аналогично происходит распознавание по рисунку вен на руке). Специально разработанная инфракрасная камера позволяет сканировать информацию для фиксированных зон лица. Система обеспечивает близкую к 100 % точность распознавания даже при проведении пластических операций, так как термограмма – это схема расположения внутренних кровеносных сосудов.

**Вывод:** Наиболее перспективными технологиями сегодня являются проксимити, СМАРТ, RFID карточки. Проксимити карточки несмотря на широкое распространение и очевидного их преимущества над магнитными и виганд-аналогами, отличаются высокой ценой и ограниченным диапазоном считывания (до 15см). У смарт-карточек тоже высокая цена, что связано с более сложной ее конструкцией и наличием встроенного микропроцессора. Однако для многих приложений эти недостатки перевешиваются следующими преимуществами: высокая защищенность и многофункциональность.

Рынок безопасности с нетерпением ожидает прорыва в области hands-free технологий, которые демонстрирует технология Radio Frequency Identification(RFID). В перспективе это позволит пользователю передвигаться по зданию, не доставая карточки. Система доступа сама будет отслеживать перемещение человека, улавливая радиосигналы крошечного транспондера на расстоянии до 4 метров. Пока внедрение RFID сдерживается дороговизной оборудования и неудовлетворительной защитой транспондеров от экранирования.

Лидерами способов идентификации являются биометрические считыватели, но они пока очень дороги, кроме того, имеют сравнительно большое время идентификации (для большого потока людей это может оказаться неприемлемым). Все биометрические считыватели не рассчитаны на уличное применение.

Т.е выбор варианта структуры СКУД неразрывно связан с требованиями к обеспечению безопасности конкретного объекта, эффективность использования любых технических средств СКУД зависит от применяемой технологии контроля доступа и квалификации оперативно-технического персонала. При выборе систем необходимо учитывать экономические показатели, поэтому для реализации учебного макета будут использоваться универсальные средства идентификации.

**1.3 Анализ и выбор исполнительных механизмов СКУД**

Если задача СКУД состоит в ограничении прохода через обычные двери, то исполнительным устройством будет электрически управляемый замок или защелка, представлен на рисунке 2. Здесь можно применить считыватели дистанционного типа с большим расстоянием считывания.

Электрические замки подразделяются на электромеханические и электромагнитные.

В электромеханических замках кроме электрической схемы присутствует механика, аналогичная механике обычного замка. Открыть такой замок можно тремя способами: ключами, механической кнопкой, расположенной на корпусе замка, или электрическим сигналом.

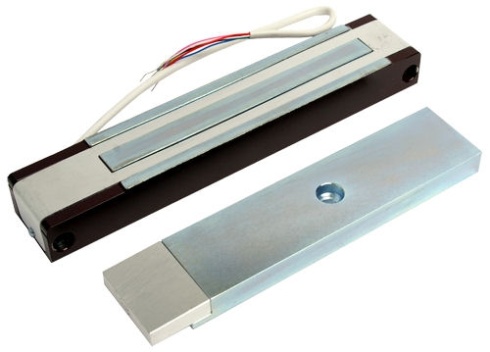


Рисунок 2 - Замок или защелка

Электромагнитные замки представляют собой мощный электромагнит. Для закрытия замка на него постоянно подается напряжение, открывание производят отключением питания (замки пригодны для установки на путях эвакуации при пожаре).

Следующим видом исполнительных устройств являются турникеты, которые бывают двух основных типов исполнения: поясные и полноростовые. Принцип действия всех турникетов примерно одинаков. Пользователь подносит к устройству считывания идентификатор, и если идентификатор действителен, турникет разблокируется. Турникеты могут быть оборудованы средствами сигнализации, срабатывающими при попытках обхода, перепрыгивании. Для этого используются ИК-барьеры, весочувствительные датчики и т. п.

Разновидности:

- трехштанговый турникет (трипод);

- роторный турникет (вертушки);

 -турникеты типа «метро»;

- калитка.

Внешний вид разновидностей исполнительных механизмов показан на рисунке 3. Ворота и шлагбаумы чаще всего используются на въездах на предприятие и на автомобильных парковках. Для этого СКУД имеют в своем составе специальные автомобильные идентификаторы, считыватели для установки под полотном дороги, дистанционные считыватели. Основное требование – устойчивость к климатическим условиям и возможность управления от контроллера СКУД.



Рисунок 3 - Внешний вид исполнительных механизмов

**Вывод:** в зависимости от типа объекта, пропускной способности, экономических показателей в системе СКУД могут использоваться разные типы исполнительных механизмов. Для практической реализации проекта - разработки действующего макета СКУД, задача которого демонстрация в ограничении прохода, исполнительным устройством выбран электромагнитный замок, он сравнительно недорогой и удобный в установке.

**1.4 Принципы работы систем контроля управления доступом**

В основе работы систем контроля и управления доступом заложен принцип сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с данными, заложенными в систему.

Каждый из пользователей получает карту доступа или брелок, содержащий индивидуальный код, присваиваемый при выдаче карты доступа. В качестве кода могут использоваться также биометрические данные человека.

При проходе на охраняемую территорию или в охраняемое помещение производится считывание данных с носителя кода через считыватели. Информация о  посетителе передается в систему, где производится анализ и дается сигнал, адекватно реагирующий на сложившуюся ситуацию: <Проход разрешен>, <Проход запрещен>, <Повторный проход по одной карте>, вывод сигнала <Тревога> на пульт охранника при нарушении охраняемой территории без соответствующих прав и т.д.

При необходимости вмешательства охраны в сложившуюся ситуацию на экран компьютера поста охраны выводится тревожный сигнал и инструкция, определяющая действия персонала в данной ситуации. Причем, система тут же может отреагировать на тревожную ситуацию, заблокировав замки в охраняемое помещение и пути прохода по точкам доступа.

Для анализа произошедших событий имеется возможность просмотра и распечатки протокола событий за определенный период времени. Для исключения злоупотреблений в  использовании карт и ужесточения проходного режима в особо важные зоны имеется ряд функций, позволяющих:

а) исключить двойной проход в зону по одной карте;

б) разрешить доступ только по 2-м картам (войти могут только два человека, встретившись вместе и обладающих соответствующими полномочиями);

в) ограничить количество лиц в помещении и зоне (при превышении установленного порогового значения контроллер не пропустит в зону очередного человека);

г) установить режим <вход под принуждением> (незаметно для окружающих охране подается сигнал тревоги);

д) охраннику дается право на самостоятельное принятие решения о разрешении на проход посетителя (при считывании карты на монитор охранника выводится фотография владельца, которая сличается с изображением, выдаваемым видеокамерой);

е) установить режим счетчика на использование карты (количество чтений карты на конкретном считывателе ограничивается);

ж) установить скрытый контроль в помещении (подать сигнал тревоги на пульт охраны при проникновении в защищаемое помещение и отсутствии  
соответствующих прав, причем для злоумышленника факт обнаружения остается неведомым).

**1.5 Классификация и обоснование выбора способа управления СКУД**

Системы контроля и управления доступом по способу управления:

1. **Автономные** – для управления одним или несколькими преграждающими устройствами без передачи информации на центральный пульт и без контроля со стороны оператора. Обычно это простые СКУД, точнее электронные замки, которые ограничивают доступ в помещения. К преимуществам таких систем можно также отнести возможность легкого удаления номера ключа из энергозависимой памяти системы при его утере, таким образом, нашедший ключ никогда не сможет им воспользоваться. Автономные системы нашли применение, как правило, на небольших объектах (входы в жилые дома, коттеджи и т.п.). Существуют и автономные системы контроля доступа с функциями охраны.

2. **Централизованные (сетевые)** – для управления преграждающими устройствами за счет обмена информацией с центральным пультом, для контроля (управления) со стороны оператора. Сетевые системы контроля применяются там, где требуется постоянный контроль состояния объекта, возможность оперативного вмешательства в работу системы и получение различных статистических данных о  движении персонала. Управление доступом в сетевых системах в основном осуществляется автоматически, на основе различных объектных и временных ограничений доступа, задаваемых как для отдельных владельцев ключей, так и для групп владельцев, выделенных по какому-либо признаку с помощью специальной программы. Оператор имеет возможность работать с базами данных пользователей, регистрировать и редактировать права доступа. При запущенной программе все события, происходящие в системе, выводятся на монитор в режиме реального времени и протоколируются для последующего получения отчетов по каждому пользователю. Система позволяет получить полный набор стандартных отчетов о  перемещениях сотрудников, а также вести учет рабочего времени. Сети связи в  системе защищены от злоумышленников аппаратно и программно. Сетевые системы оптимальны для применения в небольших и средних офисах или предприятиях (до 256 контролируемых точек прохода).

3.  **Универсальные** – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в  сетевом оборудовании, в центральном устройстве или обрыве связи.

**Вывод:** способ управления системой контроля и управления доступом выбирается по количеству контролируемых точек доступа.

**2 ПРАКТИЧЕСКОЕ ОБОСНОВАНИЕ ИССЛЕДУЕМОЙ ОБЛАСТИ**

**2.1 Аналитический обзор рынка систем контроля и управления доступом (СКУД)**

Рынок систем контроля и управления доступом (СКУД) традиционно является одним из наиболее технологичных и динамичных сегментов рынка безопасности в России.

Мы провели исследования этого рынка, в котором решались следующие задачи: охарактеризовать состояние рынка СКУД, выяснить типы СКУД, перспективные технологии СКУД, наиболее известные марки компаний производителей СКУД в Челябинской области, результаты представлены в виде диаграмм, в опросе приняли участие специалисты в области установки СКУД Челябинской области, студенты прошедшие производственную практику, а также пользователи систем.

Объем рынка систем безопасности, по данным опросов, растет. В сегменте СКУД большинство анкетируемых отметили повышение динамики роста (рисунок 4), что соответствует информации из других источников.

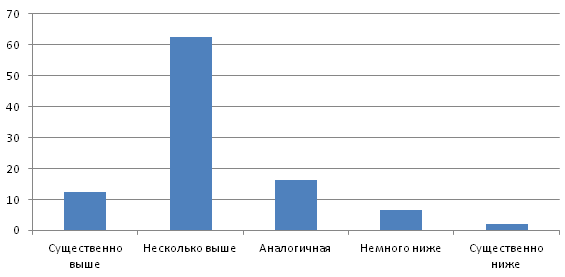


Рисунок 4 - Динамика рынка СКУД

Темпы роста в последние годы значительно выше. Во-первых, постепенно повышается информированность рынка и соответственно востребованность новых возможностей, функций и сервисов. Во-вторых, на повышение рыночной динамики значительно влияют такие факторы, как увеличение риска террористических угроз, рост общего уровня культуры потребителей.

Отдельные факторы увеличения динамики роста можно проанализировать по диаграмме на рисунке 5.

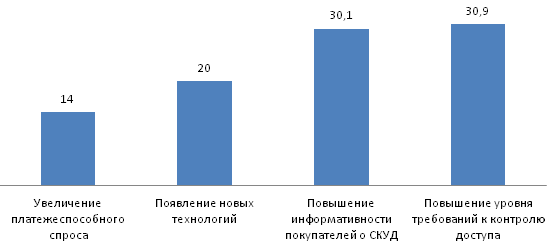
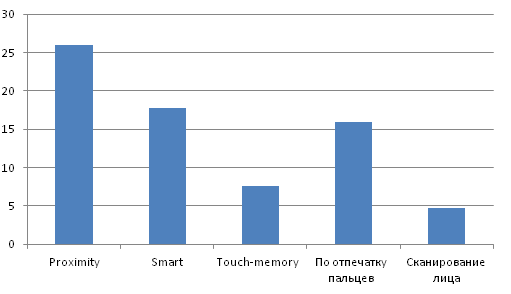


Рисунок 5 - Факторы динамики роста

В росте динамики рынка СКУД получили факторы повышения информированности потребителей и роста уровня их требований. С ростом информированности закономерно повышается уровень требований.

При определении лидеров перспективных технологий (рисунок 6) Proximity и Smart довольно близки, но по потенциалу и возможностям Smart-технология - неоспоримый лидер. Второе место биометрии, так как интерес к биометрическим технологиям на данный момент чрезвычайно высок.

  
Рисунок 6 - Перспективные технологии идентификации

На вопрос: "Какой программный продукт наиболее часто используется при применении СКУД?"(рисунок 7) оказалось что по функциональности и уровню исполнения отечественные программные продукты давно догнали, а некоторые и перегнали продукцию зарубежных производителей, отечественные программные разработки переведены на иностранные языки и успешно используются за рубежом, что говорит о высоком уровне разработки нашего ПО.

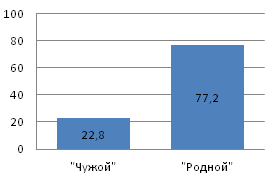


Рисунок 7 - Программный продукт при применении СКУД  
 Ближайшие перспективыв развитии рынка СКУД (рисунок 8) подавляющее большинство опрошенных назвали внедрение новых технологий, появление новых высокоэффективных и удобных технологий с богатым потенциалом будет сильно влиять на все развитие рынка СКУД.

Изменения в структуре потребителей также может сильно повлиять на рынок.

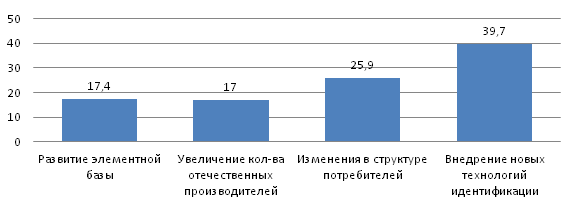


Рисунок 8 - Факторы определяющие развития рынка СКУД в перспективе

Показатель информированность потребителя представлен на рисунке 9.

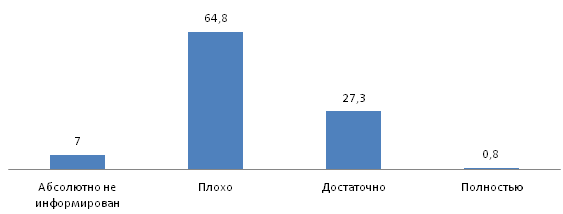


Рисунок 9 - Информированность потребителя о представленных на рынке СКУД продуктах

Кроме того выяснилось, что лишь 6% от общего количества компаний используют полностью беспроводные технологии, 17% применяют смешанные решения – комбинируют беспроводные и проводные системы, 51% использует традиционные проводные системы с картами, ключами и жетонами, 21% респондентов сообщили, что пока нет таких систем (рисунок 10).

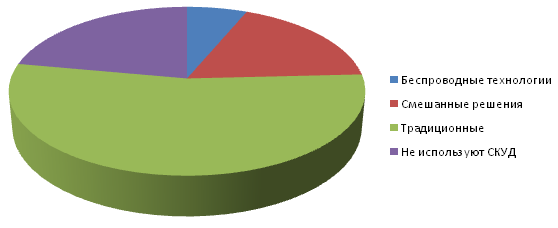


Рисунок 10 -Тип используемых технологий

Однако, по мнению каждого четвертого из пяти опрошенных (79%), на протяжении следующих нескольких лет количество применяемых СКУД как в жилых домах, так и в помещениях коммерческих организаций увеличится в разы, а на сегодняшний день проводные системы использующие карты, ключи – самые распространенные технологии.

Также в процессе исследования предлагалось ответить, СКУД каких марок им известны (рисунок 11). При ответе на данный вопрос большинство опрошенных (70%) в качестве известной им торговой марки СКУД назвали Parsec, затем были названы Болид (62%), Perco (60%), Кодос (56%)., а также другие системы.

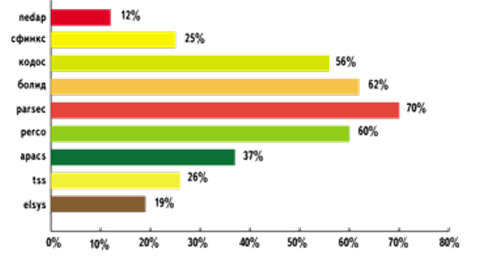


Рисунок 11 - Популярность марок СКУД

На Урале большей популярностью пользуются Болид (41%), Parsec (24%), Perco (22%) (рисунок 12).

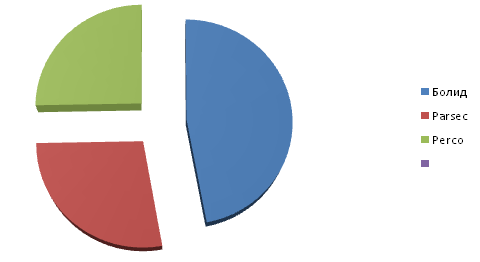


Рисунок 12 - Популярность марок на Урале

**Вывод:** в настоящее время на российском рынке имеется достаточно большой выбор систем контроля и управления доступом, как иностранного, так и российского производства, ожидается дальнейший рост, для этой динамики есть свой определяющий фактор - повышение уровня требований к контролю доступа.

Также предстоит бурное развитие биометрических технологий идентификации личности, к которым проявляется большой интерес, но выбрать этот вариант покупателю мешает малая информированность в данной области СКУД.

В целом о представленных на рынке СКУД продуктах и решениях в целом покупатель информирован достаточно хорошо, и он способен сам принимать взвешенное решение о приобретении того или иного оборудования. В наибольшей же степени на выбор СКУД влияют 3 фактора: цена, возможности и бренд.

Также исследование показало, что подавляющее большинство марок СКУД на российском рынке представлено отечественными производителями и монтажные организации отдают им безусловное предпочтение. Это можно объяснить как достаточно высокой функциональностью систем, решающих требуемые задачи безопасности, так и оптимальным соотношением цена – качество и в значительной степени доступностью сервиса (техническая поддержка, ремонт и т. п.).

**2.2 Моделирование архитектуры макета системы**

Моделирование автономной СКУД необходимо для изучения назначения, принцип действия, конструкции, схем подключения всех внешних соединений автономной СКУД на базе контроллера LC-1DW, а также получение навыков программирования и работы с СКУД во всех режимах, регулировки параметров контроллера LC-1DW.

Поэтому, чем понятнее будет действующий макет, тем проще будет расширить свои знания по исследуемой теме. Моделирование архитектуры СКУД представлено в виде взаимодействующих между собой объектов, такой подход более близок и понятен учащемуся, студенту, поскольку он наиболее удобно отражает принцип действия. Объектное мышление позволяет представлять и понимать все более сложные системы, включая биометрическую.

Оборудование, помогающие промоделировать систему, позволяет визуально изобразить объекты и их взаимодействие, последовательно изучить, продемонстрировать процесс и адаптировать его к  изменяющимся потребностям, т.е макет позволяет наглядно продемонстрировать структуру и поведение системы. Макет необходим для визуализации и управления архитектурой системы и позволяет добиться лучшего понимания систем СКУД.

Как уже отмечалось выше, в системе СКУД количество и функциональность модулей зависят от назначения системы и производителя, для разрабатываемой автономной системы обосновано и выбрано оборудование:

- контроллер – LC-1DW;

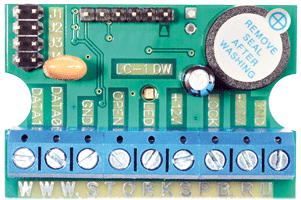
- бесконтактный считыватель –FLY ЗЕМ;

- электромагнитный замок ML -180k;

- считыватель КТМ;

- кнопка Exit;

- карта проксимити EM – marin;

- ключ DS 1990.

Автономный контроллер доступа LC-1DW показан на рисунке 13 предназначен для организации одностороннего контроля точки прохода с применением любых контактных или бесконтактных считывателей идентификационных жетонов работающих по протоколам Dallas Touch Memory и Wiegand-26. Оптимальное решение для организации СКУД начального уровня.

Особенности

1. Количество подключаемых считывателей (контактный или бесконтактный) – 1.
2. Количество подключаемых кнопок - 1.
3. Подключение и управление всеми типами замков.
4. Защита от залипания кнопки «выход».
5. Возможность переноса базы пользователей в сетевую версию СКУД.
6. Функция разблокировки дверей и звуковой индикации в случае срабатывания пожарной сигнализации.
7. Режим «Автоматическое занесение жетонов в память контроллера».
8. Компактные габариты устройства для размещения его внутри замка.
9. Увеличенное расстояние между считывателем и контроллером - до 35 м (в случае применения бесконтактных считывателей STORK - [Fly 2](http://www.storkspb.ru/5_katalog/22_beskontaktnye_schityvateli_fly/143_nastennyj__fly_a2_eh_.html) / [Fly 3](http://www.storkspb.ru/5_katalog/22_beskontaktnye_schityvateli_fly/145_nastennye_fly_a3_eh_.html)).
10. Режим работы «Триггер» - управление работой исполнительного устройства (вкл/выкл): одно касание ключа – исполнительное устройство закрыто, повторное – открыто.
11. 5 байтная защита кода жетона.
12. Простой, интуитивно понятный режим программирования.

**Возможности**

1. Программирование пользователем двух мастер-ключей.
2. Программирование с помощью мастер-ключа до 900 шт пользовательских ключей.
3. Энергонезависимая память для хранения информации о пользовательских ключах.
4. Программирование с помощью мастер-ключа времени открывания замка от 0, 5 до 127 сек, с шагом 0, 5 сек.
5. Удаление с помощью мастер-ключа всех пользовательских ключей.
6. Дополнительная возможность открывания замка с помощью кнопки «открыть».
7. Защита от статического электричества.
8. Индикация всех режимов работы (встроенный зуммер, светодиод).
9. Замена мастер-ключей без обнуления базы пользователей.
10. Обнуление базы пользовательских ключей без удаления мастер ключей.
11. Режим "Автоматическое занесение жетонов в память контроллера".
12. Каждый новый идентификатор, поднесенный к считывателю, записывается в память контроллера и одновременно инициируется режим прохода.
13. Возможность размещения в монтажной коробке EB-820 (65х65х18мм).

Технические характеристики контроллера приведены в таблице 1.

Таблица 1 - Технические характеристики

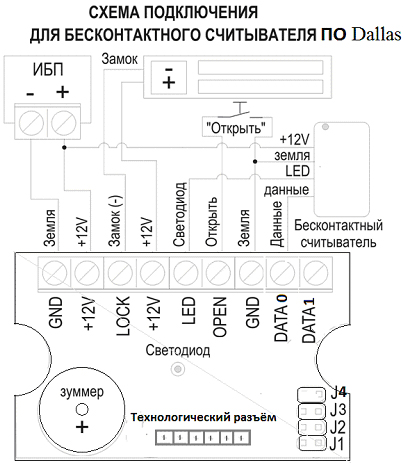
|  |  |
| --- | --- |
| Характеристика | Значение |
| 1 | 2 |
| Напряжение питания контроллера, В | 9 – 15 (DC) |
| Ток потребления контроллера при U пит. = 12: |  |
| - в режиме ожидания, мА | не более 15 |
| - в режиме коммутации, мА | не более 30 |
| Выход управления замком ток, А | не более 3 |
| Расстояние от считывателя до контроллера: |  |
| - Touch Memory при сечении кабеля 0,22 мм2, м | не более 100 |
| - Wiegand-26 при сечении кабеля 0,22 мм2, м | не более 100 |
| Количество используемых Мастер-ключей, шт. | 2 |
| Количество подключаемых считывателей, шт. | 1 |
| Количество подключаемых кнопок, шт. | 1 |
| Количество пользовательских ключей/карт, шт. | 900 |
| Тип ключей | DS1990A |
| Встроенная энергонезависимая память | EEPROM |
| Максимальное время опознавания ключа, сек. | 0,7 |
| Программируемое время открывания замка | регулируется от 1 до 127 сек. с шагом 1 сек. (по умолчанию установлено 3 сек.) |
| Перемычка для выбора типа замка | электромагнитный, электромеханический |
| Продолжение таблицы 1 |  |
| 1 | 2 |
| Рабочий диапазон температур, С | от –35 до +50 |
| Относительная влажность | не более 90% |
| Габаритные размеры (ДхШхВ), мм | 48х32х16 |

Назначение клемм приведено в таблице 2.

Таблица 2 - Назначение клемм

|  |  |
| --- | --- |
| Маркировка | Назначение |
| GND | Вход -12В питания контроллера |
| + 12V | Вход +12В питания контроллера/считывателя Fly2 EM/светодиода считывателя iButton (Touch Memory) |
| LOCK | Выход управления замком (к данной клемме подключается «Минус**»** замка) |
| LOCK+ 12V | Вход +12В питания замка (к данной клемме подключается «Плюс**»** замка) |
| LED | Выход для подключения внешней индикации считывателя (открытый коллектор транзистора с резистором 1 кОм и током не более 30мА). К данной клемме подключается «Минус**»** светодиода считывателя iButton (Touch Memory) и индикация считывателя Fly2 EM |
| OPEN | Вход «ОТКРЫТЬ» для подключения кнопки (при нажатии осуществляется замыкание на землю) |
| GND | Общий для подключения -12В считывателя Fly2 EM/кнопки |
| DATA 0 | Подключение считывателя с протоколом Touch Memory (Wiegand-26) |
| DATA 1 | Подключение считывателя с протоколом Wiegand-26 |

Разработаны схемы подключений которые приведены ниже на рисунке 14 .



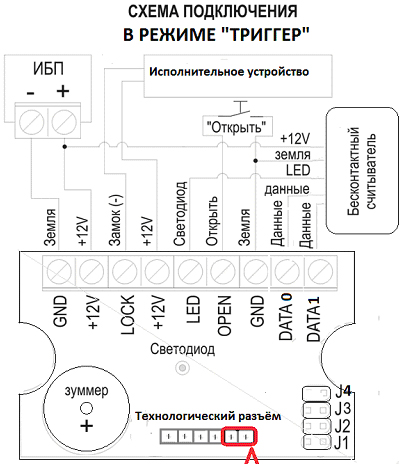
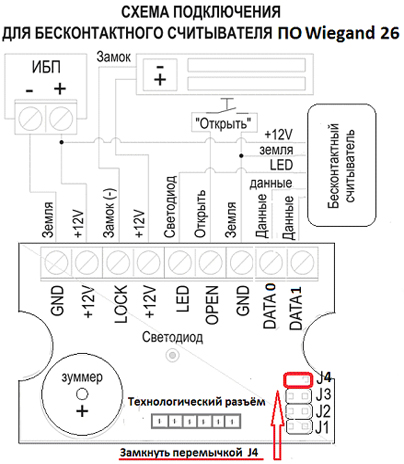


Рисунок 14 - Схемы подключений

Характеристика, назначение дополнительного оборудования:

1. Электромагнитный замок ML -180k показан на рисунке 15.



Рисунок 15 - Электромагнитный замок ML -180k

Технические данные замка приведены в таблице 3.

Таблица 3 - Технические данные

|  |  |
| --- | --- |
| Напряжение питания контроллера, В | 12,0– 14,5 |
| Потребляемый ток, А | не более 0.4 |
| Усилие держания, кг | на отрыв - 180 кг |
| Габариты (Д  Ш  В), мм | 180 x 40 x 25 |
| Масса, кг | 0.8 |

2.Считыватель КТМ-Н показан на рисунке 16.

Рисунок 16 - Считыватель КТМ-Н

Считыватель КТМ-Н предназначен для получения информации с ключа посетителя и передачи ее в контроллер для дальнейшей обработки.

Считыватель КТМ-Н представляет собой металлическую площадку с двумя контактами - один для передачи данных, другой для «заземления». Считыватель Touch Memory изготавливается из окрашенной нержавеющей стали. Он устойчив к влиянию внешней среды и не нуждается в дополнительной защите от вандализма. Габаритные размеры, Ø49×21мм Считыватель КТМ-Н оборудован светодиодом, что делает его удобным в использовании. Код ключа Touch Memory является индивидуальным и запрограммирован при его изготовлении. Считыватель, получив код, распознает его и передает контроллеру, который отвечает за дальнейшую обработку полученной информации.

Цветовая маркировка проводов:

- красный – центральный вывод контактного устройства;

- черный – общий контактного устройства;

- желтый – "плюс" LED светодиода;

- синий – "минус" LED светодиода.

3. Бесконтактный считыватель FLY представлен на рисунке 17.

Рисунок 17 - Бесконтактный считыватель FLY

Бесконтактные считыватели серии FLY предназначены для работы в составе автономных и сетевых СКД и совместимы с контроллерами, имеющими интерфейсы для подключения считывателей по протоколам Wiegand-26, TouchMemory, RS-232. Корпус считывателей серии Fly выполнен из прочного пластика ABS, электронные части устройств защищены полимерным компаундом, благодаря чему считыватели имеют высокую степень защищенности. Считыватель Fly2 EM снабжен двухцветным светодиодом и встроенным зуммером для индикации состояний системы. Технические данные считывателя приведены в таблице 4.

Таблица 4 - Технические данные

|  |  |
| --- | --- |
| Напряжение питания, В | 9 – 15 |
| Потребляемый ток, мА | 25 |
| Типы идентификаторов | EM-Marine |
| Интерфейс связи с системой (выбирается перемычкой) | Touch Memory Wiegand-26 |
| Габариты (Д ´ Ш ´ В), мм | 85х41х16 |
| Масса, г | не более 50 |

4. На рисунке 18 изображена кнопка "Выход".



Рисунок 18 - Кнопка Exit

Кнопка Exit фирмы ROSSLARE (Гонконг) наиболее часто используется для разблокировки запирающих устройств (электрозамков, электрозащелок) систем контроля доступа. Имеет нормально-замкнутые и нормально-разомкнутые контакты. Может также использоваться в контрольно-охранных системах для постановки/снятия с охраны.

5. На рисунке 19 изображена карта EM-Marine.



Рисунок 19 - Карта EM-Marine

Пластиковый пропуск использует проксимити технологию и предназначен для идентификации персонала в системах контроля доступа и учета рабочего времени. Электронный пропуск в виде пластиковой карты имеет память на 64 бит, рассчитанную на чтение без перезаписи, и может передавать идентификационный код неограниченное число раз. Такая проксимити карта работает совместно со считывателями стандарта Em Marine на частоте 125 кГц, при этом расстояние считывания кода составляет до 10 см. Карта Em-Marine ISO имеет стандартные размеры 85х54 мм, но отличается тонким корпусом - 0.8 мм.

6. На рисунке 20 изображен ключ Touch Memory.



Рисунок 20- Ключ Touch Memory

Touch Memory DS1990A-F5 - электронный идентификатор (ключ TM), который представляет собой носитель данных с уникальным кодом, предназначен для систем контроля доступа, охранных систем и других систем, где необходима идентификация. Ключ TM DS1990A является пассивным элементом (не имеет внутреннего источника питания). Держатель ключа TM выполнен в прочном корпусе с высокой стойкостью к внешним воздействиям (загрязнения, повышенная влажность и удары). Информация записывается и считывается из памяти ключа TM в память контроллера путем касания считывающего устройства. В микросхему ключа TM во время её изготовления записывается 64-разрядный код, который состоит из 48-разрядного уникального серийного номера, 8-разрядного кода семейства и 8-разрядной контрольной суммы. Ключ TM DS1990A может применяться также в системах контроля и учета рабочего времени.

**2.3 Программирование системы**

Алгоритм программирования контроллера СКУД в разных режимах:

1. Программирование контроллера с помощью Мастер-ключа.

Мастер-ключи в комплект поставки не входят и в память контроллера на заводе-изготовителе не программируются. Поэтому, при первом включении контроллер входит в режим записи Мастер-ключей. В память контроллера может быть записано только два Мастер-ключа. После записи данных ключей их необходимо хранить в безопасном месте. Второй Мастер-ключ является запасным на случай поломки первого.

Если была выполнена операция удаления Мастер-ключей из контроллера, то при первом включении контроллер так же входит в режим записи Мастер-ключей.

Мастер-ключи не открывают двери, они предназначены для программирования параметров контроллера.

Пользовательский ключ, записанный в память контроллера, не может быть запрограммирован в качестве мастер-ключа. Для его программирования в качестве мастер-ключа вначале необходимо удалить его из памяти контроллера.

Мастер-ключи запрограммированные в контроллер в режиме работы Touch Memory, не являются мастер-ключами для режима Wiegand-26 и наоборот.

Для индикации режимов программирования в считывателе Fly2 EM были задействованы выводы "BUZ" и "GREEN LED". Данные выводы подключены к клемме "LED" контроллера.

Для начала программирования контроллера выберите режим работы Wiegand-26 или Touch Memory. Протокол Wiegand-26 устакнавливается перемычкой J4 .

2.Запись Мастер-ключей в память контроллера.

Переход в данный режим осуществляется при первом включении контроллера или при его включении после процедуры удаления Мастер-ключей.

Переход контроллера в данный режим программирования индицируется равномерным миганием зеленого светодиода, периодичностью 1 раз в секунду.

Если к контроллеру подключен считыватель Fly2, переход в режим программирования, индицируется красно-зеленым миганием светодиода, сопровождающиеся прерывистым звуковым сигналом.

Внимание: Если в течение ≈ 15 сек. к считывателю не будет поднесено ни одного идентификатора (будущего Мастер-ключа), контроллер перейдет в исходное состояние. Для возврата в данный режим снимите и снова подайте питание на контроллер.

Для записи Мастер-ключей в память контроллера возьмите два идентификатора и по очереди поднесите их к считывателю. Если необходимо запрограммировать только один Мастер-ключ, поднесите идентификатор к считывателю два раза подряд.

Запись Мастер-ключа в память контроллера сопровождается подачей звукового сигнала контроллером.

При записи Мастер-ключа, считыватель Fly2 индицирует кратковременное загорание зеленого светодиода, сопровождающееся подачей одного звукового сигнала.

Завершение операции записи Мастер-ключей индицируется погасанием светодиода контроллера, пропаданием звукового сигнала считывателя и постоянным свечением красного светодиода считывателя Fly2.

3.Исходное состояние контроллера

Контроллер находится в исходном состоянии, если светодиод контроллера погашен, отсутствует звуковой сигнал считывателя Fly2 EM, а светодиод считывателя Fly2 постоянно горит красным цветом.

4.Программирование пользовательских ключей.

Убедитесь, что контроллер находится в исходном состоянии. Для перехода в режим программирования пользовательских ключей поднесите Мастер-ключ один раз к считывателю.

Переход в данный режим сопровождается двумя кратковременными звуковыми сигналами контроллера и индицируется постоянным свечением зеленого светодиода контроллера.

Индикация считывателя Fly2, в данном режиме программирования, сопровождается постоянным свечением зеленого светодиода считывателя и подачей постоянного звукового сигнала.

Для записи пользовательских ключей по очереди поднесите их к считывателю с интервалом в 1-2 секунды.

Внимание: Если в течение 1 минуты, после перехода контроллера в режим программирования Вами не будет произведено никаких действий, контроллер вернется в исходное состояние.

Запись пользовательского ключа в память контроллера сопровождается подачей звукового сигнала контроллером и кратковременным погасанием зеленого светодиода.

При записи пользовательского ключа, считыватель Fly2 индицирует кратковременное загорание красного светодиода, сопровождающееся прерыванием постоянного звукового сигнала.

По завершению операции программирования пользовательских ключей, для выхода из данного режима два раза поднеси Мастер-ключ к считывателю, после чего контроллер вернется в исходное состояние.

Внимание: Если во время программирования Вы пытаетесь повторно произвести запись уже существующего в памяти контроллера пользовательского ключа, контроллер по истечении 60 сек. вернется в исходное состояние.

5.Программирование времени открывания замка.

Время открывания замка может быть установлено в диапазоне от одной до 127 секунд, с шагом 1 секунда. По умолчанию на заводе изготовителе время открывания замка установлено равным 3 сек.

Внимание: Для данного режима программирования требуется наличие подключенной КНОПКИ к контактам OPEN и GND контроллера и считывателя для перехода в режим программирования.

Убедитесь, что контроллер находится в исходном состоянии. Для перехода в режим программирования времени открывания замка поднесите Мастер-ключ один раз к считывателю.

Переход в данный режим сопровождается двумя кратковременными звуковыми сигналами контроллера и индицируется постоянным свечением зеленого светодиода контроллера. Индикация считывателя Fly2, в данном режиме программирования, сопровождается постоянным свечением зеленого светодиода считывателя и подачей постоянного звукового сигнала. Для установки нового значения времени открывания замка нажмите и удерживайте кнопку на время, которое Вы определили как время, необходимое для открывания замка.

По наступлению требуемого времени отпустите кнопку, контроллер вновь перейдет в режим программирования времени открывания замка.  
Для выхода из данного режима поднесите Мастер-ключ два раза к считывателю, после чего контроллер вернется в исходное состояние.

6.Удаление всех пользовательских ключей из контроллера.

Для данного режима требуется наличие подключенной КНОПКИ к контактам OPEN и GND контроллера.

Убедитесь, что контроллер находится в исходном состоянии.

Для перехода в режим удаления пользовательских ключей поднести Мастер-ключ к считывателю два раза.

Переход в данный режим программирования сопровождается двумя кратковременными звуковыми сигналами контроллера и индицируется равномерным миганием светодиода контроллера, периодичностью 0,5 секунды.

Для считывателя Fly2, переход в данный режим программирования, индицируется красно-зеленым миганием светодиода считывателя. Каждое мигание сопровождается подачей прерывистого звукового сигнала.

Для запуска операции удаления пользовательских ключей нажмите кнопку и удерживайте ее больше 5 сек.

Удаление пользовательских ключей индицируется постоянным свечением светодиода контроллера и считывателя Fly2 на протяжении 3 секунд, после чего контроллер переходит в исходное состояние.

Дополнительные режимы, активируемые с помощью перемычек

Внимание: Снятие и установка перемычек должны сопровождаться снятием питания с контроллера. Допускается одновременная установка перемычек J2,J3,J4 и триггер.

7. Удаление Мастер-ключей.

Для перехода в режим удаления Мастер-ключей снимите питание с контроллера и установите перемычку J1, после чего вновь подайте питание.

Процесс удаления Мастер-ключей индицируется миганием светодиода контроллера, периодичностью один раз в секунду и сопровождается постоянным звуковым сигналом контроллера.

Процесс удаления Мастер-ключей для считывателя Fly2 индицируется красно-зеленым миганием светодиода считывателя, сопровождающиеся прерывистым звуковым сигналом.

О завершении операции удаления Мастер-ключей свидетельствует погасание светодиода контроллера, пропадание звуковых сигналов контроллера и считывателя и постоянное свечение красного светодиода на считывателе Fly2.

Для выхода из режима удаления Мастер-ключей снимите питание с контроллера и удалите перемычку J1. При последующей подаче питания, контроллер автоматически перейдет в режим программирования Мастер-ключей.

8.Установка типа замка.

Внимание: Тип замка устанавливается только при отключенном питании.

Если перемычка J2 установлена, то замок открывается снятием напряжения (электромагнитный замок, защелка нормально-открытая).

Если перемычка J2 не установлена, то замок открывается подачей напряжения (замок взводного типа, защелка нормально-закрытая).

Данный режим не имеет индикации контроллера и считывателя.

9.Автоматическое добавление пользовательских ключей.

Внимание: Будьте внимательны! При первом включении контроллера с установленной перемычкой J3, контроллер в начале переходит в режим программирования мастер-ключей, поэтому первые два ключа, поднесенные к считывателю, могут быть запрограммированы в качестве мастер-ключей. Если Вы планируете занести все ключи в качестве пользовательских, Вам необходимо дождаться завершения режима программирования мастер-ключей (≈ 60 сек. после включения питания контроллера).

Для перехода в режим автоматического добавления пользовательских ключей необходимо снять питание с контроллера и установить перемычку J3, после чего вновь подать питание на контроллер. Во время активации данного режима все ключи, поднесенные к считывателю, будут открывать дверь и одновременно записываться в память контроллера. Для выхода из режима отключите питание от контроллера и снимите перемычку J3, после чего снова подайте питание на контроллер.

10.Режим "Wiegand-26".

Для работы контроллера по протоколу Wiegand-26 снимите питание с контроллера и установите перемычку J4 (рисунок 14). Подключите к контроллеру считыватель, поддерживающий протокол Wiegand-26 используя контакты Data0 и Data1. Подайте питание на контроллер. Контроллер готов к работе в режиме Wiegand-26.

Внимание: В считывателях Fly 2 для перехода в режим Wiegand-26 необходимо «перекусить» соответствующую перемычку (см. описание на считыватель).

11.Режим "Триггер".

Данный режим необходим для управления внешними устройствами с потреблением не выше 3А и напряжением питания 12В. Управляемое устройство подключается к контактам LOCK и +12V. Для включения режима «триггер» отключите питание контроллера и установите перемычку «триггер», согласно приведенной схеме.

Внимание!

Режим триггера будет функционировать в зависимости от режима установленного перемычкой J2.

Режим триггера недопустим при работе с электромеханическими замками, защелками и т.д. — это приведет к выходу устройства из строя.

Подайте питание на контроллер. При включении режима на выходе клемм подключения управляемого устройства (LOCK, +12B) значение выходного напряжения +12В или 0 в зависимости от перемычки J2.

При прикладывании жетона, занесенного в базу контроллера, выходное напряжение становится равным 0 или +12В. При повторном прикладывании ключа, выходное напряжение снова становится равным +12В или 0.

Для выхода из режима «триггер» отключите питание контроллера и удалите перемычку «триггер». Подайте питание на контроллер.

**ЗАКЛЮЧЕНИЕ**

Целью данного проекта является анализ рынка и самих технических средств систем СКУД, разработка архитектуры макета автономной СКУД на базе контроллера LC-1DW, его практическая реализация, позволяющая предотвратить несанкционированный доступ к охраняемым объектам.

Для достижения поставленной цели были решены поставленные задачи, которые показывают что применение систем контроля управления доступом на современном этапе развития общества оправдано, ведь сфера применения достаточно широка. Она не ограничивается только крупными производственными корпорациями, но и с успехом используется в офисных помещениях.

Во-первых, вопрос идентификации пользователей актуален для любого объекта, установка системы контроля управления доступом, позволит не только поднять уровень общей безопасности, но и сократить издержки затрат на ее обеспечение, поскольку СКУД не требуют большого количества персонала для обслуживания, экономичны в потреблении электроэнергии.

Во-вторых, сегодня СКУД считается одним из самых интенсивно развивающихся направлений в безопасности, что подтверждено результатами исследования. Это связано с возможностью добиться полной автоматизации. Благодаря этому снижается влияние человеческого фактора и уменьшаются затраты, но существенным минусом к массовому внедрению приоритетных направлений, например биометрической идентификации СКУД по прежнему является экономическая составляющая.

В первой главе производится обзор предметной области, раскрываются основные понятия системы контроля управления доступом (СКУД), состав и принципы работы, изложены базовые механизмы, положенные в основу архитектуры системы контроля доступа. Проанализированы и сравнены способы идентификации, типы исполнительных механизмов СКУД, также приводится классификация СКУД, обоснование выбора типа системы контроля и управления доступом. Конкретизированы положительные и отрицательные стороны технологий систем контроля доступа.

Вторая глава посвящена практическому обоснованию предметной области исследования. В первой части с помощью анализа, сравнения, используя метод опроса и опытно-поисковой работы проведено аналитическое исследование, обработаны и представлены результаты: дана характеристика состояние рынка СКУД, выяснены типы используемых в России СКУД, перспективные технологии СКУД, наиболее известные марки компаний производителей СКУД в Челябинской области.

В процессе анализа определено, то, что для потребителей, ориентированных на безопасность, приоритетными будут современные технологии проксимити, СМАРТ, RFID карточки.

Производители продолжат осваивать потенциальные возможности беспроводных технологий. В силу низкой цены еще долгое время востребованным решением будут считаться классические технологии.

Усовершенствуются технологии защиты кодов идентификации, и увеличится дальность считывания. Расширится интеграция биометрических и RFID-технологий, в том числе предложение устройств с хранением биометрических данных на карте. Варианта выбора структуры СКУД по прежнему неразрывно связан с требованиями к обеспечению безопасности конкретного объекта.

Кроме того исследование показало, что подавляющее большинство марок СКУД на российском рынке представлено отечественными производителями и монтажные организации отдают им безусловное предпочтение. Это можно объяснить как достаточно высокой функциональностью систем, решающих требуемые задачи безопасности, так и оптимальным соотношением цена – качество и в значительной степени доступностью сервиса (техническая поддержка, ремонт и т. п.). Будет востребовано программное обеспечение (ПО), учитывающее грамотный баланс между простотой освоения и функциональностью.

Также можно сделать следующий прогноз: для крупных объектов будут востребованы широкий функционал, высокая надежность и защищенность, легкость расширения и модернизации в будущем.

Для распределенных объектов, вне зависимости от их масштаба, ключевыми будут централизация функций мониторинга и контроля, многоуровневая система резервирования, способность автономного функционирования отдельных составляющих системы.

Для небольших объектов доминировать будут автономные системы контроля, обладающие низкой ценой, простотой в управлении, установки и эксплуатации. Этим преимуществом при изготовлении макета, наглядно демонстрирующего принцип работы СКУД, мы и воспользовались в своем проекте.

В результате выполненных работ самостоятельно была разработана архитектура системы контроля управления доступом, практическая ценность реализована в виде действующего макета представленного на рисунке 21, который может быть использован в качестве базы. Макет необходим для визуализации и управления системой и позволяет добиться лучшего понимания систем СКУД.

Макет позволяет визуально изобразить объекты и их взаимодействие, последовательно изучить состав СКУД, схемы подключения всех внешних соединений автономной СКУД.

Особенностью данной разработки является использование микроконтроллера LC-1DW в качестве управляющего элемента устройства контроля и управления доступом, благодаря этому устройство обладает простотой, широкой функциональностью, а также поможет получить навыки программирования и работы с СКУД во всех режимах, продемонстрировать процесс и адаптировать его к  изменяющимся потребностям.



Рисунок 21- Фото действующего макета СКУД

Разработанный проект рекомендован для использования в учебном процессе при закрепления теоретических знаний по теме «Системы контроля и управления доступом», в получении практических навыков, программировании контроллера, изучении режимов работ контроллера. Предназначен для студентов и специалистов, а также в качестве выставочного образца в профориентационной работе учебного учреждения.

Теоретическое и практическое значение полученных результатов сопоставимо с целями и задачами проекта, данный макет будет востребован, так как имеет интуитивно понятный интерфейс, принцип работы.

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Бадагуев, Б. Т. [Электромонтажные работы и работы по монтажу, настройке и сдаче в эксплуатацию технических средств сигнализации](http://www.ozon.ru/context/detail/id/17586093/) [Текст] : практ. пособие / Б. Т. Бадагуев. – М.: Альфа-Пресс, 2012. – 288с.

2. [Ворона, В. А.](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) Инженерно-техническая и пожарная защита объектов: справочное издание [Текст] / В. А. [Ворона,](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) В. А. [Тихонов](http://www.techbook.ru/book_list.php?str_author=%D0%A2%D0%B8%D1%85%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%90.). – М.: Горячая линия-Телеком, 2012г. – 511 с. – (Обеспечение безопасности объектов ; кн. 4)

3.[Ворона, В. А.](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) Комплексные (интегрированные) системы обеспечения безопасности [Текст] / В. А.[Ворона,](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) В. А.[Тихонов](http://www.techbook.ru/book_list.php?str_author=%D0%A2%D0%B8%D1%85%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%90.). – М.: Горячая линия - Телеком, 2013. – 160с. – (Обеспечение безопасности объектов ; кн. 7).

4.[Ворона, В. А.](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) Системы контроля и управления доступом: справочное издание [Текст] : [справ. изд.] /В. А. [Ворона,](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) В. А. [Тихонов](http://www.techbook.ru/book_list.php?str_author=%D0%A2%D0%B8%D1%85%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%90.). – М.: Горячая линия - Телеком, 2015. – 272с. – (Обеспечение безопасности объектов ; кн. 2).

5.[Ворона, В. А.](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.) Теоретические основы обеспечения безопасности объектов информатизации: учебное пособие для вузов [Текст] / В. А. [Ворона](http://www.techbook.ru/book_list.php?str_author=%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B0%20%D0%92.%D0%90.), В. А. [Тихонов,](http://www.techbook.ru/book_list.php?str_author=%D0%A2%D0%B8%D1%85%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%90.) Л. В. [Митрякова.](http://www.techbook.ru/book_list.php?str_author=%D0%9C%D0%B8%D1%82%D1%80%D1%8F%D0%BA%D0%BE%D0%B2%D0%B0%20%D0%9B.%D0%92.); под ред. В. А.[Тихонова,](http://www.techbook.ru/book_list.php?str_author=%D0%A2%D0%B8%D1%85%D0%BE%D0%BD%D0%BE%D0%B2%20%D0%92.%D0%90.) Л. В. [Митряковой.](http://www.techbook.ru/book_list.php?str_author=%D0%9C%D0%B8%D1%82%D1%80%D1%8F%D0%BA%D0%BE%D0%B2%D0%B0%20%D0%9B.%D0%92.) – М.: Горячая линия -Телеком, 2015. – 304с.

6. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний [Текст]. – Взамен ГОСТ Р 51241-98: введ. 30.06.1989. – М.:Стандартинформ, 2009. – 31 с.

7. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения [Текст] : учеб. пособие / И. И. Груба. – М.: Солон-Пресс, 2012. – 220с. – (Библиотека инженера).

8.Михайлов, Ю. Б. Научно-методические основы обеспечения безопасности защищаемых объектов [Текст] / Ю.Б.Михайлов. – М.: Горячая линия - Телеком, 2015. – 322 с.

9. Рекомендации. Выбор и применение систем контроля и управления доступом [Электронный ресурс]: Р 78.36.005-2011 // Техэксперт: новигатор в мире ГОСТов : справочная правовая система. – Режим доступа: Компьютерная сеть библиотеки «ЮУрГТК» (дата обращения: 18.02.2016).

10.Рекомендации. Выбор и применение систем контроля и управления доступом [Электронный ресурс]: Р 78.36.002-2010 // Техэксперт: новигатор в мире ГОСТов : справочная правовая система. – Режим доступа: Компьютерная сеть библиотеки «ЮУрГТК» (дата обращения: 18.02.2016).

11.Биометрическая идентификация и аутентификация [Электронный ресурс]. - Режим доступа: http://www.gmmcc.com.ua // ?id=76. - Название с экрана.

12. Интегрированные системы безопасности [Электронный ресурс]. - Режим доступа: http://www.aamsystems.ru/publications/?id=132. - Название с экрана.

13. Биометрические системы контроля доступа [Электронный ресурс]. - Режим доступа: http://ien.izi.vlsu.ru/teach/books/910/theory.html#\_1. - Название с экрана.

14. Контроль доступа: устройства контроля доступа ведущих мировых производителей [Электронный ресурс]. - Режим доступа: http://www.armosystems.ru/system/hid\_skd.ahtm. - Название с экрана.