Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

ВНЕДРЕНИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА В СВЕРДЛОВСКОМ ОТДЕЛЕНИИИ СБЕРБАНКА

Дипломная работа
ДР 08080165.103

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ Н.С. Толстова
«___» _____ 2016 г.

ВНЕДРЕНИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА В СВЕРДЛОВСКОМ ОТДЕЛЕНИИ СБЕРБАНКА

Дипломная работа
ДР 08080165.103

Исполнитель:
студент группы Кп-511 ИЭ А.С. Вахрушев
Руководитель:
ст. преподаватель кафедры ИС С.В. Ченушкина
Нормоконтролер:
ст. преподаватель кафедры ИС Е.В. Зырянова

РЕФЕРАТ

Пояснительная записка к дипломной работе выполнена на 75 листах машинописного текста, содержит 24 рисунка, 5 таблиц, 25 источников литературы.

Ключевые слова: СИСТЕМА КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ, БЕЗОПАСНОСТЬ, ВНЕДРЕНИЕ.

Объект исследования – Свердловское отделение №7003 ПАО Сбербанк.

Предмет исследования – внедрение единой системы контроля доступом на объектах Свердловского отделения Сбербанка.

Цель дипломной работы – выбрать и внедрить в Свердловском отделении Сбербанка централизованную систему контроля и управления доступом с учетом особенностей предприятия и его инфраструктуры.

Для достижения поставленной выше цели, были решены следующие **задачи**:

- рассмотреть основные возможности систем контроля доступом;
- проанализировать представленные на рынке системы контроля и управления доступом;
- проанализировать существующее состояние пропускных систем на различных объектах предприятия заказчика;
- выбрать и обосновать методологию внедрения системы на предприятии;
- рассчитать экономическое обоснование проекта и примерную смету внедрения.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Как любой театр начинается с вешалки, так и любая система информационной безопасности начинается с обеспечения физической безопасности самой информационной системы независимо от её вида, размера и стоимости. В физической безопасности термин «контроль доступа» относиться к практикам ограничения доступа к собственности, в здания или помещения, доступ к которым разрешён только для авторизованных людей. Физический контроль доступа, может быть, достигнут путём использования человека (охранник, вышибала или служащий в приёмной), через механические способы, такие как замки и ключи на двери, или через технологические средства, такие как системы доступа, основанные на картах доступа или биометрической идентификации.

Очевидно, что для того, чтобы обеспечить безопасность домашней информационной системы, необходимо, по крайней мере, запирать двери на ключ перед уходом. В большинстве компаний, которые используют информационные системы для работы, на входе, если не в рабочее помещение, то в здание находится специально обученный человек с надписью «охрана» или «служба безопасности» на бейдже или на спине, который обычно требует предъявить пропуск тех, кто работает в этом здании и записывает в журнал всех, кто не работает в этом здании/помещении, но по каким-то деловым вопросам должен пройти внутрь. По легенде делает он это для того, чтобы можно было в случае утери имущества быстро найти того, кто мог это сделать из посторонних. Как правило, современные офисные помещения снабжены камерами видеонаблюдения, поэтому в случае неправомерных действий посетителей их можно будет легко идентифицировать. В идеале возле каждой двери в помещение должен сидеть специально обученный охранник, сверять пропуска и записывать в журнал кто, в какое время входил и выходил.

Помимо охранника двери в помещения нужно закрывать на замки. Если с замками всё более или менее понятно, то с охранниками, которые аккуратно фиксируют в журнал каждое открывание двери, обычно проблемы даже не успевают возникнуть, т. к. слишком нерентабельно содержать такую армию людей не занятных в непосредственном рабочем процессе компании, который приносит основную прибыль.

Для того чтобы уменьшить издержки на охранном персонале и повысить уровень физической безопасности применяют системы контроля и управления доступом (в здания и помещения).

Многообразие производителей оборудования для организации пропускного режима, различные конфигурации и возможности расширения и интеграции могут ввести неподготовленного заказчика в ступор. Зачастую не решает проблему множество монтажных фирм.

Свердловское отделение № 7003 это одно из 4 отделений входящих в состав территориального Уральского банка ПАО Сбербанк, которому принадлежит сеть объектов по г. Екатеринбургу. При этом каждый из них имеет свою систему управления доступом, и возникает необходимость постоянного обеспечения работников идентификаторами СКУД для разных объектов.

Для повышения безопасности было принято решении о внедрении на крупных объектов, где располагаются несколько структурных подразделений единую централизованную СКУД.

Объектом исследования в данной дипломной работе является Свердловское отделение №7003 ПАО Сбербанк.

Предметом исследования является внедрение единой системы контроля и управления доступом на объектах Свердловского отделения Сбербанка.

Цель работы – выбрать и внедрить в Свердловском отделении Сбербанка централизованную систему контроля и управления доступом с учетом особенностей предприятия и его инфраструктуры.

В соответствии с поставленной целью в работе определены следующие **задачи**:

1. Рассмотреть основные возможности систем контроля доступом.

2. Проанализировать представленные на рынке системы контроля и управления доступом.

3. Проанализировать существующее состояние пропускных систем на различных объектах предприятия заказчика.

4. Выбрать и обосновать методологию внедрения системы на предприятии.

5. Рассчитать экономическое обоснование проекта и примерную смету внедрения.

1 АНАЛИЗ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

1.1 Определение и основные возможности систем контроля и управления доступом

Перед началом анализа существующих систем контроля и управления доступом (СКУД), необходимо дать определение понятию СКУД.

Согласно ГОСТ Р 54831-2011 «Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний» [4]. СКУД – это совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Такая формулировка не дает нам понимания всей картины рассматриваемого понятия. Если рассмотреть более обширно СКУД - совокупность совместимых между собой аппаратных и программных средств, направленных на ограничение и регистрацию доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

В большинстве случаев СКУД включает:

- устройства преграждающие управляемые (УПУ). Например, турникеты, двери, оборудованные управляемыми замками, ворота, шлагбаумы, шлюзы;
- устройства считывающие (УС), «считыватели». Например, устройства радиочастотной идентификации, дактилоскопические сканеры, устройства машинного зрения;
- контроллеры СКУД. Электронные микропроцессорные модули, реализующие аутентификацию объектов доступа, логику авторизации для доступа в те или иные помещения и области, управление УПУ;

- программное обеспечение СКУД. Необязательный элемент, позволяющий осуществлять централизованное управление контроллерами СКУД с персонального компьютера (ПК), формирование отчетов, разнообразные дополнительные функции;
- конверторы среды для подключения аппаратных модулей СКУД друг к другу и к ПК;
- вспомогательное неинтеллектуальное оборудование (блоки питания, кнопки), соединительные провода.

Одним из важных понятий для понимания работоспособности СКУД является идентификатор доступа, или идентификатор (носитель идентификационного признака): уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код (рисунок 1). Идентификатор, использующий вещественный код - предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и др. устройства) [20].

В условиях индивидуальных особенностей экономических субъектов рассматривать возможности СКУД необходимо дифференцируя потребности каждого. Анализируя потребности банков/офисов можно выделить индивидуальные аспекты малозначимые для промышленных предприятий/заводов и государственных объектов. Тем не менее, всем СКУД присущи базовые функции, включенные в систему по умолчанию [21]:

- ведение и поддержание баз данных пользователей и карт/идентификаторов;
- хранение фотографий пользователей в базе данных;
- фиксация даты и времени прохода в базе данных;
- задание уровней доступа;
- автономная работа контроллеров системы с сохранением основных функций управления при нарушении связи с компьютером;

- регистрация и хранение информации о событиях в энергонезависимой памяти контроллеров СКУД;
- сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;
- открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;
- запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака.

Рисунок 1 – Методы идентификации

Рассмотрим дополнительные функции, которые, так или иначе, важны для всех потребителей [14]:

1. Учет рабочего времени. С помощью программной надстройки СКУД позволяют работодателю учитывать время выхода персонала на работу и ухода с неё. Кадровые работники или специально назначенные сотрудники могут точно определить время пребывания сотрудника на рабочем месте. В начале дня встроенная в СКУД система учета рабочего времени позволяет формировать отчет о сотрудниках, не прошедших через точки доступа. Функция упрощает процедуры выявления опаздываю-

щих или не вышедших на работу сотрудников. Это позволяет выявлять опоздавших или не явившихся на рабочее место сотрудников. Гибкость программных аналитик СКУД позволяет менеджменту формировать необходимые отчеты.

2. Возможность аппаратной и программной интеграции, регистрация и протоколирование событий в подсистемах ОПС и CCTV. Основной смысл интеграции – это в первую очередь объединение отдельных подсистем с помощью единого интерфейса, который позволял бы выполнять и мониторинг, и настройку системы «из одного окна». Таким образом, взаимная интеграция различных систем безопасности существенно облегчает работу служб безопасности, снижает время реакции на внештатные ситуации, а также повышает эффективность ведения расследования происшествий на объекте. Интеграция данных систем безопасности на аппаратном уровне имеет смысл в тех случаях, когда на объекте уже есть установленное оборудование и интегрировать его с новыми системами на программном уровне не представляется возможным. Кроме того, в случае оснащения небольших офисов аппаратная интеграция систем безопасности может обеспечить финансовую экономию, поскольку закупать крупную комплексную систему и ПО будет просто невыгодно.

3. Наличие SDK (Software Development Kit) для доработки функционала. Очень часто требования заказчика к комплексу систем безопасности простираются гораздо шире, чем могут предложить готовые и отработанные решения. В таких случаях приходится интегрировать большое количество разрозненных подсистем, и здесь, конечно же, не обойтись без SDK. В качестве примера систем, для интеграции которых необходим SDK, можно привести ERP-систему предприятия, систему выдачи ключей от помещений, а также ИТ-инфраструктуру организации, которая позволяет объединить логический и физический доступ.

4. Проход «с подтверждением» со стороны оператора. Такая функция СКУД весьма востребована на проходной, когда охранник контроли-

рует проход и выполняет фотоверификацию сотрудника по изображению, которое система выдает на монитор оператора при поднесении к считывателю карты доступа. Помимо непосредственной визуальной верификации в рамках этой функции может быть выполнено сравнение фотографий с видеопотоком, который система выдает на рабочую станцию оператора.

5. Доступ по правилу «два лица и более». Это правило является востребованным при ограничении доступа в спецпомещения. Кроме того, в СКУД Lenel существует такое понятие, как «хозяин зоны», то есть в случае его отсутствия доступ в зону будет запрещен кому бы то ни было. Обычно это и подобное ему правило «эскорт» применяются в банковских СКУД.

6. Вход в режиме «шлюз». Организация шлюзов бывает необходима при построении системы контроля доступа в особо важные помещения или здания, такие как банковские хранилища и дата-центры. В зависимости от архитектурных особенностей объекта, а также от финансовых возможностей заказчика можно как установить готовую шлюзовую кабину, так и выполнить шлюз в виде тамбура, ограниченного двумя дверьми со считывателями на вход и на выход (бюджетный вариант).

7. Защита техсредств и ПО от НСД. Защита от несанкционированного доступа к настройкам оборудования и ПО СКУД является необходимым условием надежной и эффективной работы системы, не позволяет допускать нарушения условий допуска и работы персонала.

8. Управление объектами с распределенной филиальной структурой. Наличие системы удаленных филиалов (особенно для банков и крупных корпораций) является обычной организационной структурой, при этом наличие унифицированной на всю филиальную систему СКУД повышает надежность и удобство мониторинга и управления бизнес-процессами. Многоорганизационность (то есть функционирование в рамках одной системы ряда «автономных», невидимых друг другу, кроме

единого управляющего центра, систем) – крайне актуальна именно для бизнес-центров с множеством арендующих офисы организаций.

9. Подключение считывателей различных типов. Часто в требования проектировщика и конечного заказчика по дизайну и ряду функций входит подключение к единой СКУД считывателей различных производителей, а в ряде случаев и различных способов идентификации (RFID, биометрия и т.п.).

10. Ручное, полуавтоматическое или автоматическое открывание УПУ при ЧС. Данная функция является необходимым условием эксплуатации объектов и помещений по технике безопасности.

11. Управление работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т.п.). Данная функция повышает уровень автоматизации объекта, позволяет значительно сократить издержки на обслуживающий и контролирующий персонал – в общем, управлять всеми инженерными системами с одного пульта, унифицировать архивы событий по всем системам и привязывать их к единой базе данных персонала.

12. Максимальное количество идентификаторов для точки прохода. Понимается количество карточек, которые могут быть записаны на одном контроллере. Наиболее узким местом являются контроллеры турникетов на центральной проходной, так как через нее ходят все сотрудники и посетители. Для обычного офисного здания это ограничение не играет большой роли (число сотрудников и посетителей редко превышает несколько тысяч). Однако если речь идет о предприятии с несколькими корпусами и большим количеством сотрудников, этот параметр необходимо учитывать.

13. Максимальное количество контроллеров в сети. Фактически означает максимальное количество контролируемых точек прохода в системе. Выбирая СКУД для установки, необходимо учитывать, что в дальнейшем систему, возможно, придется масштабировать. И если система

«вырастет» из максимального количества контроллеров, то встанет вопрос о её децентрализации.

1.2 Общие принципы работы

Существующие системы контроля доступа (СКД), условно, можно разделить на две категории:

1. Простые, рассчитанные всего на одну входную дверь. Обычно при такой архитектуре используются автономные контроллеры
2. Сложные, предназначенные для контроля доступа на крупных объектах - предприятиях, заводах и банках [19].

Независимо от конфигурации СКУД, каждая подобная система состоит из нескольких обязательных узлов, это - контроллеры для управления, считыватели для идентификации, а также всевозможные исполнительные устройства ограничения доступа: турникеты, электромагнитные замки и защелки. Электронные бесконтактные карты в качестве пропусков являются самым распространенным и удобным средством идентификации в системах контроля доступа.

Принцип работы всех систем сводиться к трем базовым действиям:

1. Предоставление права доступа.
2. Идентификация.
3. Доступ.

Работает система контроля и управления доступом следующим образом: после установки системы контроля доступа на объекте, каждый сотрудник получает уникальный идентификатор (магнитная карточка, бесконтактная карта, отпечаток пальца, в случае использования биометрических систем) и выставляются права доступа в различные зоны. На входе в зоны, требующие контроля, устанавливаются считыватели идентификаторов, контроллеры и электромагнитные замки. При подносе идентификатора к считывателю, считыватель передает информацию контроллеру, который определяет, имеет

ли данный идентификатор право допуска в служебное помещение, и при наличии соответствующих прав открывает доступ (рисунок 2). Если используется функция учета рабочего времени, то в базу данных вносится соответствующая информация о событии [15].

Идентификатор может одновременно является пропуском на территорию организации и ключом от помещений, куда сотруднику разрешен доступ.

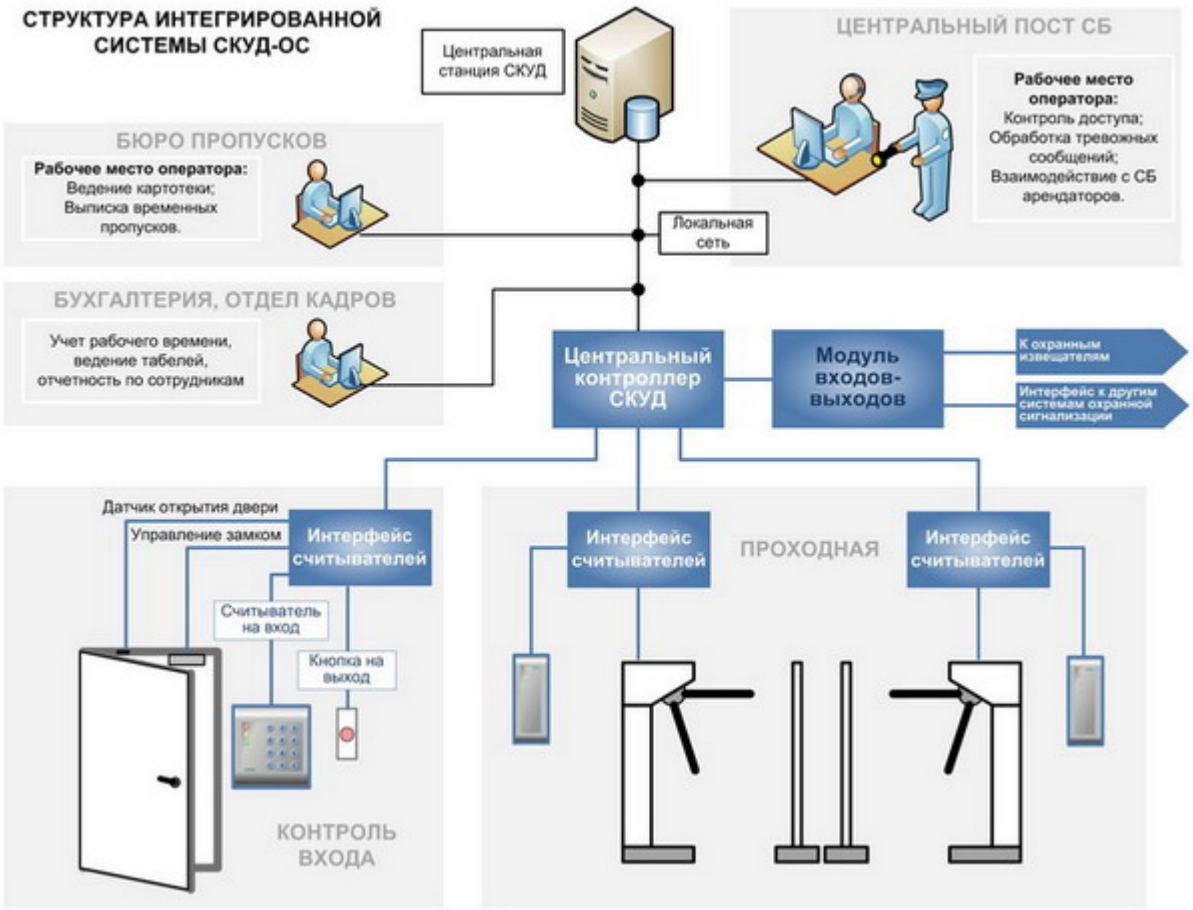

Рисунок 2 – Схема работы СКУД

Все ограничивающие устройства подключаются к контроллерам системы управления доступом. Контроллеры предназначены для приема и анализа информации о предъявляемых картах доступа, а также для управления различными исполнительными устройствами. В состав оборудования системы контроля доступа могут входить два типа контроллеров: контроллеры замка и контроллеры турникета, каждый из которых отвечает за контроль работы собственного узла.

Для прохода через турникет или входа в ответственное помещение работники предприятия должны поднести свою карту доступа к считывателю, после чего считыватель передает код предъявленной карты в контроллер, а контроллер доступа принимает решение о разрешении или запрете прохода на основании заложенной в него информации. В случае если доступ разрешен, система контроля доступа автоматически разблокирует турникет или замок на двери (рисунок 3).

Рисунок 3 – Идентификация пользователя

Также с помощью СКУД можно осуществлять контроль въезда автотранспорта на территорию объекта, в этом случае после предъявления персонального идентификатора происходит открытие ворот или подъем шлагбаума (рисунок 4).

Рисунок 4 – Идентификация для допуска автотранспорта

Для организации групповых политик контроллер СКУД может быть запрограммирован на пропуск конкретных сотрудников в определенные помещения только в заданные промежутки времени.

Все события о проходах через контрольные пункты фиксируются в памяти системы управления доступом и могут использоваться для автоматизированного учета рабочего времени, блокировок учетных записей во внутренней компьютерной сети, а также для получения отчетов по дисциплине труда или для возможных служебных расследований на предприятии.

1.3 Обзор источников по системам контроля и управления доступом

В книге «Системы контроля и управления доступом» [3] изложен широкий круг вопросов, связанных с организацией контрольно-пропускного режима на различных объектах и применением СКУД. Большое внимание уделено средствам идентификации и аутентификации. Описаны устройства идентификации (считывания) различных типов; средства биометрической аутентификации личности и особенности их реализации; различные виды контроллеров и исполнительные устройства СКУД. Приведен обзор различных вариантов реализации СКУД. Даны основные рекомендации по выбору средств и систем контроля доступа. В приложении приведены ключевые выдержки из официальных нормативных материалов связанных с использованием СКУД.

В книге «Системы безопасности и устройства кодового доступа. Просто о сложном» [10] приведены описания стандартов в спецификациях Международного комитета по стандартизации ISO 18902, ISO 7816, ISO 14443 варианты A и B, ISO/IEC 15693, 180 15693-2, спецификации EMV (Europay, MasterCard, Visa), IPC/JEDEC J-STD-020C, ECMA 340, ETSI TS 102190 и др. Системы, работающие по технологии Java, регламентируются и описываются в стандартах Java Card 2.1.1, Java Card 2.1.1 и выше. Рассмотрены технические характеристики наиболее популярных микроконтроллеров, которые мо-

гут пригодиться разработчикам и пользователям систем безопасности и кодового доступа. Собраны актуальные сведения по новейшим системам доступа и безопасности, конфигурации систем СКУД, рассмотрены особенности «меток» различных стандартов, их технические характеристики и справочные данные по микроконтроллерам смарт-карт. В третьей главе книги представлены новые радиолюбительские схемы и избранные электронные устройства-помощники по теме охраны и контроля доступа.

В книге «Электронная идентификация» [6] рассматриваются актуальные вопросы создания и применения электронных идентификационных средств для обеспечения достоверности учета и контроля во всех сферах жизнедеятельности человека. Подробно анализируются технологии бесконтактной радиочастотной идентификации с индуктивной, электромагнитной и емкостной связью между мобильными носителями электронных данных и считывающими устройствами. Рассматриваются перспективные системы электронной идентификации, основанные на использовании эффекта поверхностных акустических волн. Значительное внимание уделяется таким перспективным средствам электронной идентификации, как интеллектуальные смарт-карты. Описываются принципы, современные алгоритмы и протоколы криптографической защиты электронных идентификаторов, в частности смарт-карт. Приводятся многочисленные примеры практического применения средств электронной идентификации в разнообразных областях жизнедеятельности человека.

Учебное пособие «Системы контроля и управления доступом» [2] рассматривает безопасность и защиту информационных ресурсов, материальных ценностей и коммерческой тайны, дисциплину сотрудников как совокупность необходимых условий нормального существования и успешного развития любого предприятия. Авторами рассматриваются системы контроля и управления доступом. Анализируются особенности функционирования, основные характеристики и параметры, которые целесообразно учитывать при

проектировании системы, выборе алгоритма ее работы и конкретной аппаратуры для реализации.

Учебное пособие «Проектирование и исследование комплексных систем безопасности» [17] рассматривает все компоненты обеспечения безопасности. Автор детально описывает каждую составляющую. Проводит обзор, в том числе устройств идентификации, видов исполнительных устройства и контроллеров СКУД. Дается оценка влияния СКУД на обеспечение безопасности объекта.

1.4 Технология внедрения системы контроля и управления доступом

Внедрение СКУД в организации многостадийный процесс, который не ограничивается только техническими мероприятиями. Более того, без достаточно глубоко проработанной идеологии построения системы не стоит принимать технические решения. Рассмотрим основные этапы построения СКУД с точки зрения организационных мероприятий.

1. Осознание потребности. Прежде всего руководство компании должно осмыслить необходимость внедрения СКУД, проанализировать задачи, которые могут быть решены при использовании системы, оценить уровень затрат на внедрение и эксплуатацию и сопоставить эти затраты с предполагаемой выгодой. Такая предварительная оценка может служить основанием как для принятия принципиального решения о создании системы, так и для первоначальной выработки технических требований.

2. Назначение ответственных. После принятия принципиального решения очень важно определить руководителя/координатора проекта и синхронизировать его понимание задачи с пониманием руководства. Впоследствии именно у этого человека будет «болеть голова» по поводу правильного воплощения идеи.

3. Постановка задачи на внедрение и выбор подрядчика. Следующий шаг – формальное описание задачи на основании проведенного анализа.

Такое описание может представлять собой короткий (на 2-3 страницы) документ, позволяющий потенциальному подрядчику оценить перспективы участия в проекте и подготовить черновое коммерческое предложение.

При построении системы заказчику необходимо не допустить ключевой ошибки, когда выбор идеологи и технической реализации выстраивается «от подрядчика». Другими словами, сначала на горизонте появляется «подрядчик» (чаще всего, выбранный субъективно), который предлагает и, в общем-то, навязывает идеологию и технические решения, исходя из своих возможностей и опыта. При этом такие решения далеко не всегда являются оптимальными в конкретной ситуации.

Вообще, выбор подрядчика это один из ключевых моментов построения любой технической системы, и СКУД здесь – не исключение. Чем более тщательным будет процесс выбора, тем меньше проблем возникнет в ходе реализации проекта, и тем больше он будет отвечать изначальным ожиданиям. В государственных структурах такой выбор осуществляется при помощи тендера, что не всегда приводит к оптимальному результату, поскольку определяющим критерием является стоимость. Тем не менее, при подготовке закупочной документации необходимо в требованиях детально прописать квалификационные требования к участником процедуры. Стоит уделить этому этапу достаточно времени. Впоследствии это минимизирует риск выбора недобросовестного подрядчика.

Частные же компании могут себе позволить, не инициируя громоздкие тендерные процедуры, подобрать подрядчика в короткий срок и исходя из здравого смысла.

Процесс выбора подрядчика в простом случае может выглядеть следующим образом:

- выбор предполагаемых подрядчиков (3-5 компаний);
- ознакомление предполагаемых подрядчиков с описанием задачи;
- взаимодействие с подрядчиками (ознакомление с объектом, уточнение условий);

- разработка подрядчиками коммерческих предложений;
- анализ коммерческих предложений заказчиком;
- принятие решения на основании комплексной оценки.

Для проведения комплексной оценки может быть разработана и использована сравнительная таблица (таблица 1), обобщающая полученную информацию о потенциальных подрядчиках.

Таблица 1 – Сравнительная таблица подрядчиков

Наименование	Сигма+	ТрансВидео	.....	ООО «Авось»
Телефон, e-mail	322-2332	123-4567	.....	999-9999
Контактное лицо	Иванов Иван	Петрова Людмила	.....	Сидоров Александр
Скорость реагирования	Отл.	Хор.	.....	Уд.
Качество реагирования	Отл.	Хор.	.....	Уд.
Заинтересованность	Уд.	Хор.	.....	Отл.
Адекватность понимания задачи	Отл.	Хор.	.....	Неуд.
Вариативность предложений	Хор.	Уд.	.....	Уд.
Наличие сертификата производителя оборудования	Да.	Да.	.....	Нет.
Размер компании-подрядчика	Отл.	Хор.	.....	Уд.
Стоимость решения		Хор.	.....	Отл.
Качество решения (класс оборудования)	Отл.	Уд.	.....	Уд.
Уровень ранее реализованных проектов	Отл.	Уд.	.....	Уд.
Качество оформления коммерческого предложения	Отл.	Хор.	.....	Уд.
Наличие собственного штата монтажников	Да.	Нет	.....	Да.
Наличие у монтажников сертификатов и лицензий	Да.	Нет.	.....	Нет.

Некоторые критерии в таблице могут показаться несущественными, но, например, по скорости реагирования на заявку можно сделать предположение о соблюдении сроков работ, а большой размер компании-подрядчика может гарантировать непрерывность работ при проблемах с монтажниками или быструю замену оказавшегося неисправным оборудования. Применение подобной таблицы поможет формализовать принятие решения. В крупной компании, имеющей множество объектов, когда необходимость в принятии

решений существует постоянно, целесообразно усилить степень формализации принятия решений, используя весовые коэффициенты по каждому критерию для принятия окончательного решения. Разумеется, российская действительность вносит свои коррективы в процесс выбора в сторону значительного увеличения доли субъективности, однако, если, все же, руководствоваться не желанием личного обогащения или удобства, а интересами компании, следует использовать в работе формализованные методы принятия решения.

4. Утверждение проектной и сметной документации, заключение договора. Окончательно определившись с исполнителем работ по внедрению СКУД, можно вплотную приступать к подробному взаимодействию с ним. Взаимодействие это начинается с детальной корректировки предварительно оговоренной схемы, уточнения концепции и конкретного оборудования. При обсуждении идеологии системы, опыт подрядчика может оказаться неоценимым, ведь далеко не всегда заказчик четко представляет, как будет функционировать система, с какими нюансами ему придется столкнуться в процессе эксплуатации. Поэтому важно на данном этапе получить от подрядчика максимально подробную информацию. Не последнюю роль в уточнении спецификации оборудования, количества и расположения точек доступа и, соответственно, перечня работ, играет финансовый вопрос. Минимизировать затраты можно не только путем уменьшения объемов оборудования и Работ, но и за счет некоторого (некритичного) снижения качества или надежности оборудования. На этом же этапе проговариваются места размещения центрального, оконечного и вспомогательного оборудования. Не менее важно уделить внимание документальному оформлению принятых решений. В процессе обсуждения может показаться, что сторонами достигнуто полное взаимопонимание, и необходимость в подробном документировании принятых решений отсутствует. Однако, такая ситуация может доставить массу неприятностей, если досконально не зафиксировать все договоренности документально. Нет ничего более мучительного для заказчика, чем работать по формальному до-

говору или вообще без него. Такие вещи обычно снижают общую первоначальную стоимость системы, но могут значительно увеличить ее уже в процессе монтажа. Как правило, все технические особенности проекта прописываются в ТЗ (Техническом Задании). Техническое Задание может быть как отдельно на проектирование, так и на систему в целом. Обычно ТЗ пишет исполнитель работ и согласовывает его с заказчиком в виде приложения к договору. Такая ситуация логична, поскольку подрядчик по определению профессионал в этом вопросе. Задача заказчика здесь – не поддаться соблазну формального изучения ТЗ и подробнейшим образом проверить документ на соответствие утвержденным решениям.

После утверждения проекта, до начала монтажных работ, необходимо решить ряд организационных моментов:

- помещение для монтажников;
- временный склад для оборудования. Обеспечение сохранности оборудования;
- вопросы допуска монтажников на объект и контроля;
- вопросы оперативного взаимодействия с бригадой монтажников и головной организацией;
- координация взаимодействия монтажников и эксплуатирующего объект подразделения.

5. Контроль монтажных работ. Параллельно с сопровождением работ по монтажу оборудования, целесообразно начать разработку внутренних регламентирующих документов. Даже если в компании уже действует Регламент контрольно-пропускного режима, обязательно необходимо внести в него изменения, касающиеся СКУД [18].

6. Разработка внутренних нормативных документов и регламентов. Разработка регламента пропускного режима в компании индивидуальный процесс, но в каждом должны быть должны быть отражены следующие положения:

- цели и задачи;

- точки доступа;
- порядок назначения уровней доступа;
- порядок выдачи пропусков;
- порядок выдачи гостевых пропусков;
- порядок изъятия пропусков;
- действия при утере пропуска;
- нештатные ситуации;
- формы заявок, внешний вид пропусков, формы отчетных документов.

Кроме разработки регламента, необходимо провести еще ряд организационных мероприятий, например, разработка и согласование дизайна пропусков, консультации с отделом персонала по организации взаимодействия и т.п.

7. Пуско-наладка и ввод системы в эксплуатацию. После завершения монтажных работ подрядчик проводит пуско-наладку системы. На этом этапе необходимо плотно подключить к процессу сотрудников, которые будут непосредственно эксплуатировать систему. Сотрудники должны пройти теоретическое обучение, а также, участвуя в процессе пуско-наладки приобрести практические навыки. На этом же этапе проводится ввод базы данных сотрудников в систему, назначение уровней доступа, привязка уровней доступа к конкретным сотрудникам, изготовление пропусков, выдача пропусков сотрудникам.

Ввод системы в эксплуатацию может проходить поэтапно, чтобы не вносить резких изменений в бизнес-процессы компании.

Резюмируя вышесказанное, можно утверждать, что наиболее заинтересованной стороной при введении СКУД на предприятии является заказчик, поэтому подробное участие заказчика во всех процессах разработки системы и плотное взаимодействие с подрядчиком необходимо для успешного внедрения СКУД.

1.5 Обзор существующих систем и целесообразность приобретения

Многообразие имеющихся на рынке производителей СКУД обусловлено попыткой удовлетворить множество потребностей заказчиков. У каждого производителя свое направление деятельности по функционалу оборудования и программного обеспечения. Кто-то предлагает большие, сложные системы, поддерживающие интеграцию с пожарными системами, системами видеонаблюдения, и т.д., а кто-то имеет направленность на небольшие здания и помещения с небольшим числом сотрудников.

При таком разнообразии производителей и значительном количестве характеристик оборудования покупателю достаточно сложно выбрать продукт, который ему подходит. Поэтому приходится либо обращаться к консультантам, либо выбирать то, что более понравилось внешне.

В большинстве случаев заказчик может ознакомится с основными возможностями систем использую информацию представленную на официальных сайтах производителей. Не маловажную помощь при выборе и обзоре конкретной системы оказывают специализированные издания.

Так в журнале «Директор по безопасности» [25] проведен обзор и сравнительная характеристика представленных на рынке СКУД. На основе бизнес-кейса, приближенного к реальной ситуации, проанализированы основные технические и программные возможности большинства продуктов.

Рассмотрим характеристики наиболее мощных, с точки зрения возможностей расширения и интеграции в автоматизированные системы предприятия, СКУД представленных на рынке.

OnGuard: интегрированная система безопасности компании Lenel для высотных зданий и организаций с территориально распределенными офисами [11]. Отличительная особенность системы OnGuard компании Lenel Systems International – это комплексное решение по обеспечению безопасности офисных зданий компаний с численностью от 100 до 100 000 человек, когда работа разных компонентов системы осуществляется с единой базой дан-

ных, с едиными исходными программными кодами и используется единый графический интерфейс для всех приложений. При этом интегрированная система безопасности Lenel легко масштабируется: все составные части платформы OnGuard могут работать в условиях как небольших, так и очень крупных предприятий, а купив изначально один модуль для системы контроля доступа (СКД), потребитель всегда может дополнить его системой видеонаблюдения, охранной, пожарной сигнализацией и др. охранными системами. Кроме того, платформа OnGuard имеет открытую архитектуру, поэтому для предприятий, имеющих удаленные филиалы, возможен централизованный контроль региональных систем через LAN/WAN. Схема расширения СКУД на базе OnGuard представлена на рисунке 5.

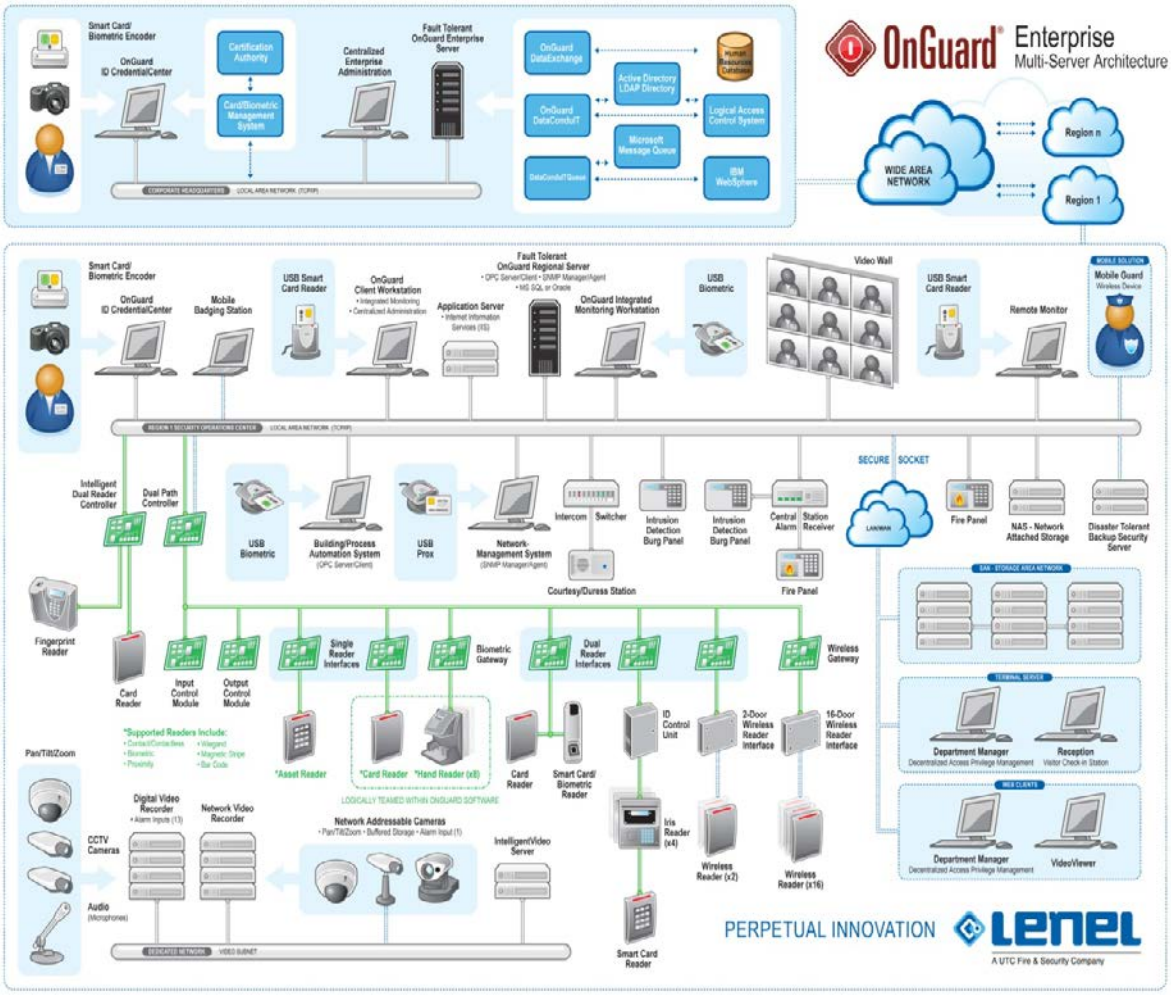

Рисунок 5 – Схема расширения СКУД OnGuard

Система централизованного контроля доступа WIN-PAK PRO Central Station от компании honeywell предлагает экономичное и легко управляемое решение для коммерческих предприятий и возможность получения регулярного дохода для компаний-установщиков систем безопасности [1]. Основные преимущества:

- реализация облачной модели предоставления приложения для системы контроля и управления доступом;
- снижение стоимости системы, увеличение количества клиентов;
- снижение расходов на установку, обучение персонала и обслуживание системы;
- средоставление дополнительных услуг, продлевающих сотрудничество подрядчика с заказчиками;
- пользователи могут управлять своими системами через веб-интерфейс.

Общий принцип работы системы представлен на рисунке 6.

Рисунок 6 – Принцип работы СКУД WIN-PAK PRO Central Station

ИСО «Орион» компании Болид - это не только СКД [7]. Система представляет собой наиболее универсальный аппаратно-программный комплекс среди представленных на рынке. Комплекс позволяет в рамках единого информационного пространства строить взаимодействующие системы охранной и пожарной сигнализации, пожарной автоматики, СКД, видеонаблюдения и диспетчеризации. В основе архитектуры ИСО «Орион» заложен модульный принцип. Система состоит из множества распределяемых по защищаемому объекту взаимозаменяемых приборов, которые, в зависимости от проведенных на этапе наладки настроек, решают одну или несколько из указанных выше задач. В качестве транспортного уровня единого информационного пространства системы в основном используются RS-485 интерфейс и сети Ethernet. Кроме того, существуют решения по организации беспроводных линий связи.

Внедрение СКД на базе ИСО «Орион» позволит решить три основные задачи:

1. Организация контроля перемещения персонала.
2. Организация охраны предприятия.
3. Организация учета.

Схема работы ИСО «Орион» представлена на рисунке 7.

Рисунок 7 – Схема работы ИСО «Орион»

Проанализируем основные технические параметры, переставленные в таблице 2.

Таблица 2 – Сравнительная характеристика технических характеристик СКУД

Параметр	OnGuard	WIN-PAK PRO Central Station	ИСО «Орион»
Макс. количество идентификаторов для точки прохода	12500	65 500	8192
Макс количество контроллеров в сети	Не ограничено	1000	32 385
Макс. количество пользователей в системе	Не ограничено	Не ограничено	64 897
Зональный antipassback	Есть	Есть	Есть
Интерфейс подключения контроллеров	Ethernet, RS-485	Ethernet, RS-485	Ethernet, RS-485
Максимальная длина магистрали до контроллера	1219м	1219м	1200м
Наличие временных зон	Есть	Есть	Есть

Несмотря на незначительные различия рассматриваемые СКУД похожи. Следует отметить, что большинство производителей СКУД не предлагает типовых решений. Архитектура конкретного проекта основывается на потребностях заказчика. В большинстве случаев на рынке предлагается оборудование, позволяющее конструировать системы под любые нужды.

Вывод

Рассмотрев функциональные возможности СКУД, требования к ним, оценив методы идентификации можно сделать вывод, что СКУД это система, основная задача которой управление доступом на заданную территорию, включающая возможности разграничения прав доступа, позволяющая проводить идентификацию пользователя и включающая дополнительные аналитические функции.

Совокупность различных методов идентификации позволяет организовать максимальный уровень защиты объекта от несанкционированного доступа. Выбор методов должен основываться на уровне секретности помещения, в которое предоставляется доступ.

Подбор компонентов системы СКУД должен основываться на потребностях заказчика, необходимости интеграции с имеющимися автоматизированными системами управления предприятием и системами безопасности.

Несмотря на схожесть функциональных возможностей для внедрения выбрана СКУД OnGuard компании Lenel. Главными факторами являются наличие ядра системы, опыт эксплуатации и администрирования. При этом отсутствие потребности для формирования базы данных позволяет достигнуть экономии финансовых и трудовых ресурсов, а наличие интеграции с автоматизированной системой учета персонала сократит время на актуализацию списка пользователей.

2 ВНЕДРЕНИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ПРЕДПРИЯТИИ

2.1 Описание предприятия заказчика

Рассмотрим заказчика внедряемой системы. Приобретение и установка оборудования производится для Свердловского отделения № 7003 ПАО Сбербанк. Сбербанк сегодня - это кровеносная система российской экономики, треть ее банковской системы. Это мощный современный банк, который стремительно трансформируется в один из крупнейших мировых финансовых институтов. В последние годы Сбербанк существенно расширил свое международное присутствие. Помимо стран СНГ (Казахстан, Украина и Беларусь), Сбербанк представлен в девяти странах Центральной и Восточной Европы (Sberbank Europe AG, бывший Volksbank International) и в Турции (DenizBank) [8].

Только в России у Сбербанка более 110 миллионов клиентов - больше половины населения страны, а за рубежом услугами Сбербанка пользуются около 11 миллионов человек. На долю лидера российского банковского сектора по общему объему активов приходится 28,7% совокупных банковских активов (по состоянию на 1 января 2016 года).

Банк является основным кредитором российской экономики и занимает крупнейшую долю на рынке вкладов. На его долю приходится 46% вкладов населения, 38,7% кредитов физическим лицам и 32,2% кредитов юридическим лицам.

Стремясь сделать обслуживание более удобным, современным и технологичным, Сбербанк с каждым годом все более совершенствует возможности дистанционного управления счетами клиентов. В банке создана система удаленных каналов обслуживания, в которую входят:

- онлайн-банкинг «Сбербанк Онлайн» (более 13 млн активных пользователей);
- мобильные приложения «Сбербанк Онлайн» для смартфонов (более 1 млн активных пользователей);
- SMS-сервис «Мобильный банк» (более 17 млн активных пользователей);
- одна из крупнейших в мире сетей банкоматов и терминалов самообслуживания (более 86 тыс. устройств).

Филиальная сеть Сбербанка состоит из 14 территориальных банков и более 16 тысяч дополнительных офисов по всей стране, в 83 субъектах Российской Федерации, расположенных на территории 11 часовых поясов.

Свердловское отделение № 7003 это одно из 4 отделений входящих в состав территориального Уральского банка ПАО Сбербанк. Помимо рассматриваемого отделения в структуру Уральского банка входят Башкирское, Челябинское и Курганское отделения, которые расположены на территории соответствующих субъектов Российской Федерации. Структура Уральского банка представлена на рисунке 8.

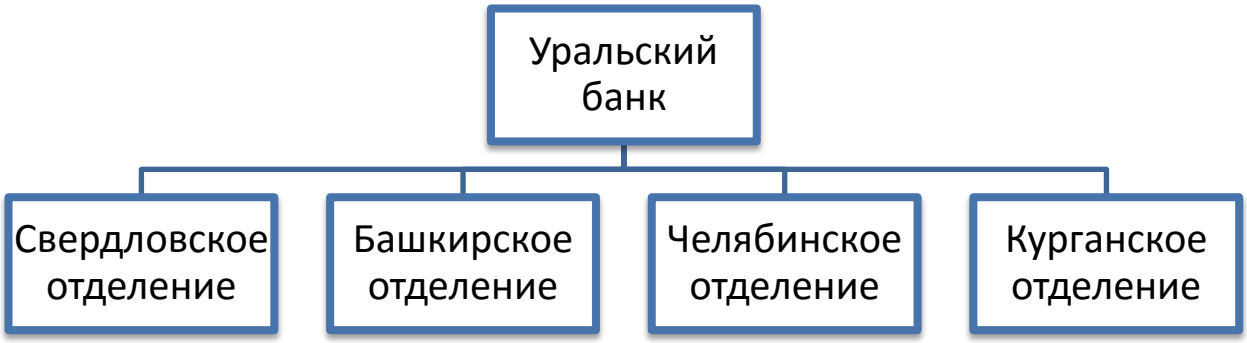

Рисунок 8 – Структура Уральского банка ПАО Сбербанк

Сегодня на базе Уральского банка в Екатеринбурге создан целый финансовый кластер: помимо головного офиса и обширной филиальной сети, в него входят Межрегиональный центр андеррайтинга, Управление регионального контактного центра, Центр сопровождения клиентских операций (рисунок 9).

Рисунок 9 – Здание Центра сопровождения клиентский операций

Сбербанк является крупнейшим эмитентом дебетовых и кредитных карт. Совместный банк, созданный Сбербанком и BNP Paribas, занимается POS-кредитованием под брендом Cetelem, используя концепцию «ответственного кредитования».

В структуру Свердловского отделения входят: одно отделение 4 уровня, расположенное в городе Нижнем Тагиле. Более 500 дополнительных офисов (Включая передвижные пункты кассовых операций) расположенных на территории Свердловской области. Парк устройств самообслуживания насчитывает более 2700 аппаратов. Свердловское отделение – это штат более 5000 сотрудников.

2.2 Анализ существующего состояния

В условиях нестабильной экономической обстановки, высокого уровня конкуренции на рынке, заказчик (Сбербанк) постоянно меняется и на первый план выходит обеспечение удобства пользователей, основная часть которых

бизнес подразделения. Выполнение одно из положений мисси банка – «Лицом к клиенту» требует от его подразделений динамических преобразований, в том числе и по изменению места нахождения офисов.

Такая динамика неизменно связана с необходимость постоянного обеспечения работников идентификаторами СКУД для разных объектов. Иным методом обеспечения является внедрение на крупных объектов, где располагаются несколько структурных подразделений централизованной СКУД.

Основные проблемы текущей эксплуатации связаны:

- с необходимостью поддержания баз данных пользователей в актуальном состоянии на всех объектах;
- с потребностью обеспечения транспортных расходов для доставки администратора системы;
- разнородностью применяемых идентификаторов;
- отсутствием возможности централизованного контроля пропускного режимов.

При этом реализуются риски утери идентификаторов пользователей, их компрометации. Зачастую сотрудники носят имеющиеся электронные ключи СКУД одной связкой и в случае утери требуется оперативный выезд на объект для блокировки.

Для создания СКУД с единым местом администрирования и обеспечивающим указанные объекты необходимо подобрать компоненты, имеющие возможность работать с сетями передачи данных (Ethernet).

В рамках этапа внедрения для монтажа системы были выбраны следующие объекты:

- административное здание (ул. Московская, 11);
- административное здание (ул. Малышева, 31в);
- административное здание (ул. Тверитина, 34);
- административное здание (ул. Ясная, 4).

Расположение офисов в г. Екатеринбурге представлено на рисунке 10.

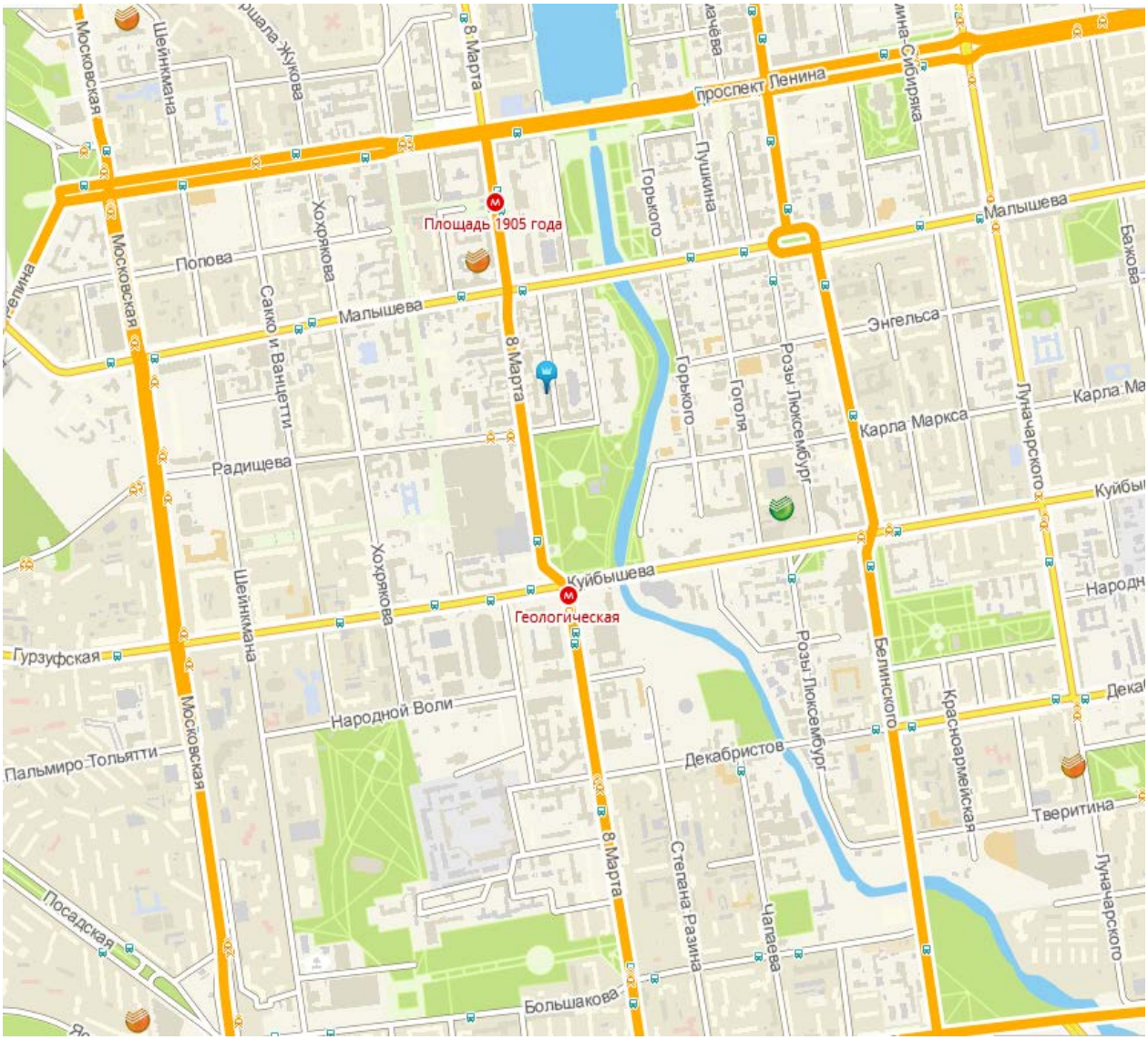

Рисунок 10 – Расположение офисов заказчика

Текущее состояние систем СКУД подразумевает установку на каждом объекте индивидуального сервера с базой данных пользователей. Администратор системы вынужден поддерживать в актуальном состоянии, и синхронизировать пользовательские данные в каждом здании. Территориальное распределение задний формирует потребность многократных выездов и соответственно трудовых затрат и издержек на транспортное обеспечение. Принципиальная схема работы СКУД в зданиях представлена на рисунке 11.

Для формирования описания проблемы необходимо рассмотреть особенности и техническое обеспечение каждого из объектов.

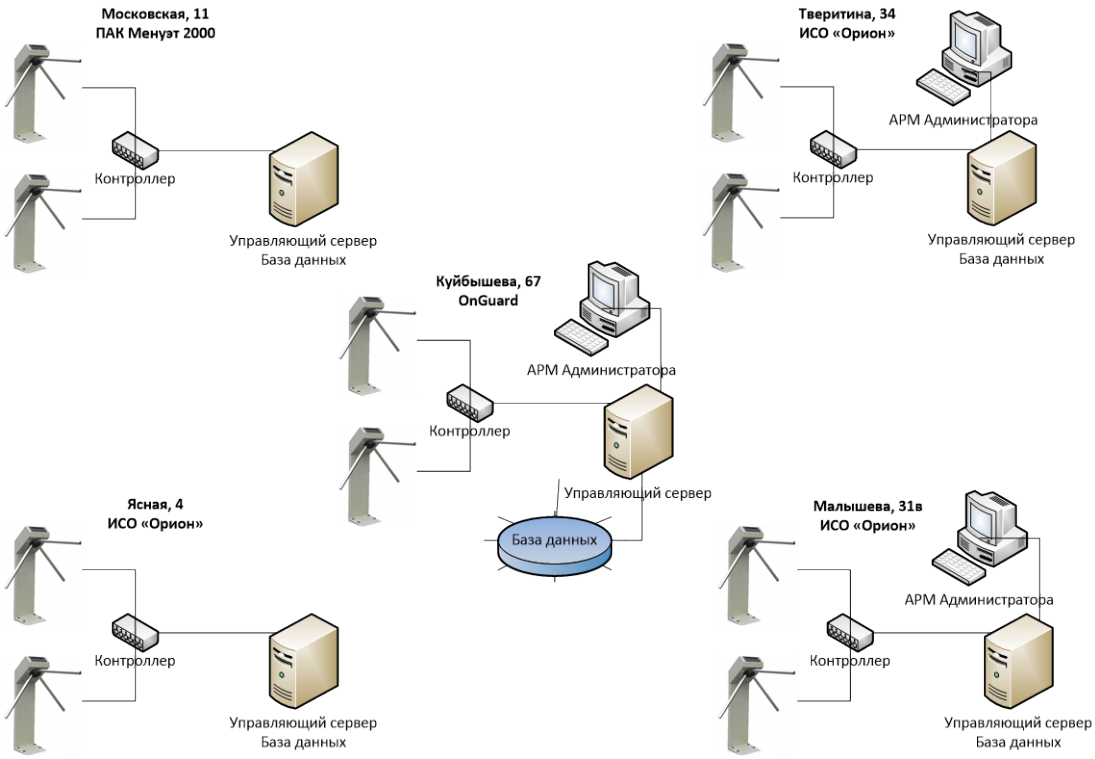

Рисунок 11 – Принципиальная схема работы СКУД

Административное здание Свердловского отделения (ул. Московская, 11). Внешний вид представлен на рисунке 12.

Рисунок 12 – ул. Московская, 11

Отделение занимает 7 этажей центрального подъезда. В задании также расположены офис ОАО «Ростелеком», Федеральной Антимонопольной Службы, РОСАВТОДОРА и д.р. компаний.

На площадях, которые занимает банк, расположены его руководство структурные подразделения аппарата отделения, дополнительный офис и центр эмиссии банковских карт. Имеются помещения для совершения операций с ценностями, серверные, кроссовые, помещения безопасности банка.

Ранее до 2012 года указанные помещения занимал территориальный банк. После реорганизации и создания на территории Свердловской области одноименного отделения аппарат территориального банка переехал в здание на улице Куйбышева, 67, а помещения вместе с инфраструктурой переданы для эксплуатации отделению.

До решения о создании Свердловского отделения предполагалось, что аппарат территориального банка переедет в новое здание, а большинство помещений будут реализованы. Финансирование в технические средства безопасности было сокращено, объем позволял только обеспечить устойчивую работоспособность.

В 2000 году при вводе в эксплуатацию здания бал смонтирован Программно-аппаратный комплекс «Менуэт 2000», который предназначен для управления доступом на предприятии [16]. На момент начала эксплуатации рассматриваемая СКУД обладала передовыми технологиями и позволяла автоматизировать процесс допуска сотрудников в помещения.

В настоящее время ПАК «Менуэт 2000» морально и физически устарел. Техническое сопровождение и модернизация, в связи с ликвидацией предприятия изготовителя, не осуществляется. База данных системы устанавливается на компьютер под управлением операционной системы Windows 95-98, материнская плата должна иметь не менее двух свободных слотов ISA. Немаловажным ограничением является количество пользователей (750) на один контроллер.

Административное здание (ул. Малышева, 31 в). Внешний вид представлен на рисунке 13.

Рисунок 13 – ул. Малышева, 31 в

Четырех этажное историческое здание банка. Является памятником архитектуры и включено в перечень объектов культурного наследия [12]. Построено в 1939 году по проекту архитектора Е.Н. Короткова. С этого здания начинается развитие сберегательного банка на Урале.

В настоящее время в здании расположены дополнительный офис, подразделения аппарата отделения, резервный вычислительный центр территориального банка.

Для контроля доступа на объект используется СКУД на базе компонентов ИСО «Орион». Срок эксплуатации системы 5 лет.

Административное здание (ул. Тверитина, 34). Внешний вид представлен на рисунке 14.

Трех уровневое здание со сложной планировкой, в котором расположены дополнительный офис, подразделения аппаратов отделения и территориального банка, а также работают сотрудники Многофункционального центра Свердловской области [13].

Для контроля доступа на объект используется СКУД на базе компонентов ИСО «Орион». Срок эксплуатации системы 9 лет.

Рисунок 14 – ул. Тверитина, 34

Административное здание (ул. Ясная, 4). Внешний вид представлен на рисунке 15.

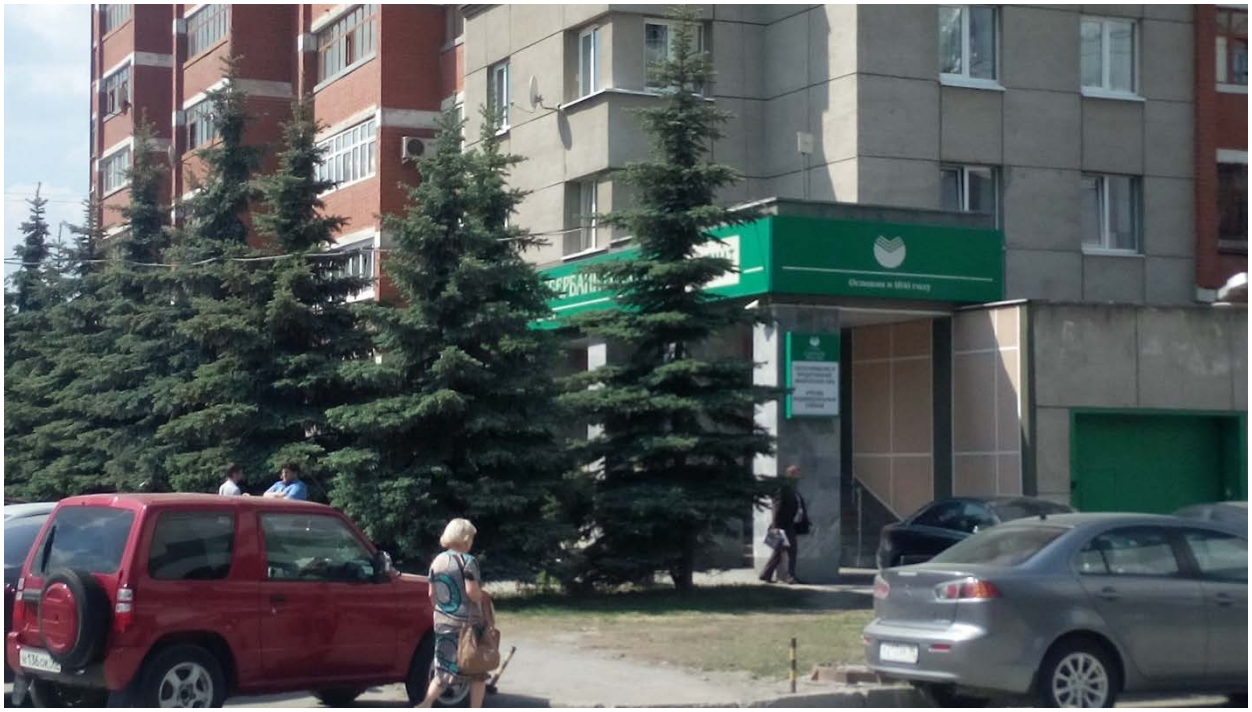

Рисунок 15 – ул. Ясная, 4

Одноэтажное здание со сложной планировкой, в котором расположены дополнительный офис и подразделения аппарата отделения. Примечательным является размещения в здании основной площадки центра удаленного мониторинга, обеспечивающего безопасность банкоматов и круглосуточных зон самообслуживания.

Для контроля доступа на объект используется СКУД на базе компонентов ИСО «Орион». Срок эксплуатации системы 12 лет.

Не маловажным фактором, влияющим на стратегию развития систем безопасности, и необходимость изменений является расположенный в городе Екатеринбурге офис территориального банка. Внешний вид здания территориального банка представлен на рисунке 16.

Рисунок 16 – Здание территориального банка

Соседство и наличие кроссфункциональных процессов, единство сетевого и серверного пространства обуславливает необходимость создания централизованных систем.

Здание оборудовано современными средствами охраны, видеонаблюдения и СКУД OnGuard компании Lenel, что является основой требований для формирования технического задания.

2.3 SWOT-анализ деятельности организации

Для выявления сильных и слабых сторон в деятельности организации с целью приспособления к изменяющимся возможностям и угрозам внешней среды был проведен SWOT-анализ.

SWOT-анализ – это определение сильных и слабых сторон процесса, а также возможностей и угроз, исходящих из его ближайшего окружения (внешней среды). Сильные стороны (Strengths) – преимущества; слабости (Weaknesses) – недостатки; возможности (Opportunities) – факторы внешней среды; использование которых создаст преимущества на рынке, угрозы (Threats) – факторы, которые могут потенциально ухудшить положение на рынке.

К преимуществам SWOT-анализа относятся:

1. Возможность использовать внутренние сильные стороны или отличительные преимущества организации в стратегии развития.

1. Возможность анализа потенциально сильных сторон и использование их для достижения маркетинговых целей.

2. Выявление слабых и уязвимых мест компании, для выяснения их влияния на положение на рынке, возможности корректировки.

3. Обнаружение ресурсов для получения максимально благоприятных результатов.

4. Выявление угроз, которые являются наиболее критичными для компании.

Проведение SWOT-анализа осуществляется заполнением «матрицы SWOT-анализа». В соответствующие ячейки матрицы необходимо занести сильные и слабые стороны рассматриваемого процесса, а также возможности

и угрозы. Данным методом проанализируем текущий процесс администрирования СКУД (таблица 3).

После централизации процесса администрирования потенциальные внутренние слабости должны превратиться в потенциальные внутренние сильные стороны, а потенциальные внешние угрозы – в потенциальные внешние благоприятные возможности.

Таблица 3 – SWOT-анализ ситуации до централизации администрирования СКУД

Потенциальные внутренние сильные стороны (S)	**Потенциальные внутренние слабые стороны (W)**
1. Знание администратором СКУД разнообразного программного обеспечения.	1. Невозможность оперативного администрирования. 2. Большие транспортные издержки. 3. Ведение баз данных пользователей на каждом объекте. 4. Отсутствие своевременного контроля действий пользователей. 5. Необходимость приобретения расходных материалов.
Потенциальные внешние возможности (O)	**Потенциальные внешние угрозы (T)**
1. Единое программное обеспечение. 2. Минимизация транспортных издержек. 3. Сокращение времени на администрирование. 4. Минимизация риска компрометации электронных идентификаторов. 5. Минимизация риска компрометации учетных записей пользователей во внутренней сети банка. 6. Автоматизация процесса актуализации базы данных пользователей. 7. Интеграция СКУД с автоматизированными системами банка.	1. Совершение противоправных действий в отношении банка. 2. Выход из строя устаревшего оборудования

Проведем SWOT-анализ после внедрения централизованного СКУД, проанализировав изменения сильных и слабых сторон, возможностей и угроз (таблица 4).

Проанализировав результаты в матрицах, можно сделать вывод, что положительный эффект внедрения информационной системы очевиден, поскольку увеличивается количество внутренних сильных сторон, уменьшается

количество внутренних слабых сторон, повышается устойчивость системы к внешним угрозам.

Таблица 4 − SWOT-анализ ситуации после централизации администрирования СКУД

Потенциальные внутренние сильные стороны (S)	**Потенциальные внутренние слабые стороны (W)**
1. Минимальные транспортные издержки. 2. Возможность удаленного администрирования. 3. Автоматизированный процесс актуализации базы данных пользователей. 4. Интеграция СКУД в автоматизированными системы банка. 5. Современное оборудование	1. Необходимость приобретения расходных материалов.
Потенциальные внешние возможности (O)	**Потенциальные внешние угрозы (T)**
1. Возможность расширения системы. 2. Возможность автоматического учета рабочего времени сотрудников банка.	• Нестабильность курса валют.

2.4 Описание выбранной методологии внедрения с учетом специфики предприятия

Монтаж систем контроля доступа – это на сегодняшний день наиболее эффективный способ осуществления безопасности как отдельного помещения, так и целого предприятия.

Задачи, которые должна решить система контроля и управления доступа:

- контроль перемещения сотрудников Банка с целью предотвращения их несанкционированного выхода, поддержания дисциплины и организации эффективного труда. Осуществляется с помощью индивидуального устройства (электромагнитного ключа или карты), которое активирует, дверь или турникет и позволяет сотруднику попасть на работу;
- автоматизацию учёта рабочего времени персонала, в результате чего использование автоматизированная система учета персонала позво-

лит для определенной группы сотрудников обрабатывать данные о фактическом количестве отработанных часов в учетном периоде;

- минимизацию риска несанкционированного доступа к информационным системам банка для уволенных сотрудников и сотрудников находящихся в отпуске;
- создание единого информационного пространства и единства подходов к обеспечению пропускного режима.

Статус заказчика – филиала публичного акционерного общества с контрольным пакетом акций принадлежащих государству [9] накладывает законодательные требования к формам выбора подрядных организаций.

При проведении закупок заказчик руководствуется требованиями:

- Гражданского кодекса Российской Федерации [5];
- Федерального закона от 26.07.2006 №135-ФЗ «О защите конкуренции» [24];
- Федерального закона от 18.07.2011 №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» [23];
- Федерального закона от 05.04.2013 №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [22];
- внутренними нормативными документами и технологическими схемами.

Сложная схема взаимодействий подразделений, необходимость множественных согласований и сложная организационная структура накладывают ограничения на детализацию плана мероприятий.

Монтаж СКУД осуществляется в несколько этапов, которые сопряжены с решением сетевых и электротехнических задач, поэтому доверять подобные работы можно только настоящим профессионалам.

Возглавляет процесс внедрения отдел технических средств охраны управления безопасности Свердловского отделения № 7003, специалисты которого имеют опыт монтажа, настройки и эксплуатации различных моделей

СКУД. Большинство сотрудников отдела начинали свою трудовую деятельность с должности монтажников, знают основы электротехники, построения слаботочных систем, имеют соответствующие. Часть сотрудников продолжила трудовую деятельность в отделе после окончания службы в правоохранительных органах.

Согласование финансовой составляющей обеспечивается «офисом финансового директора». Настройки сетевого оборудования будут обеспечиваться специалистами управления технических средств и телекоммуникаций «Центр». При необходимости общестроительных работ, предоставления доступа к инженерным системам будет привлекаться административное управление.

Согласно методологии были следующие этапы.

Этап 1. Проектирование

Сроки: 1, 2 кварталы 2016 года.

Участники: Отдел технических средств охраны управления безопасности Свердловского отделения № 7003, ООО «АРМО-Урал».

Установка СКУД начинается с анализа имеющейся структуры Банка, территориального распределения подразделений, обследования помещений и составления рабочего проекта, в котором указывается весь комплекс работ по монтажу системы, приводятся соответствующие схемы расположения замкового оборудования, производится согласование с заказчиком.

Этап 2. Подбор оборудования

Сроки: 1, 2 кварталы 2016 года.

Участники: Отдел технических средств охраны управления безопасности Свердловского отделения № 7003, ООО «АРМО-Урал».

В зависимости от типа охраняемого объекта, особенностей организации труда, требований внутриобъектового режима и структуры системы происходит подбор оптимального оборудования, способного эффективно функционировать в единой СКД.

Этап 3. Монтаж СКУД

Сроки: 3 квартал 2016 года.

Участники: Победитель закупочной процедуры, Отдел технических средств охраны управления безопасности Свердловского отделения № 7003.

Специалисты компании победителя в установленные договором сроки должны обеспечить монтаж СКУД в полном соответствии с проектом. Приобретённые компоненты системы устанавливаются подрядчиком

Этап 4. Тестирование и обслуживание

Сроки: 3, 4 квартал 2016 года.

Участники: Победитель закупочной процедуры, Отдел технических средств охраны управления безопасности Свердловского отделения № 7003.

Настройка и ввод системы в эксплуатацию обеспечивается поэтапно. После окончания монтажных работ на объекте, специалисты компании подрядчика при содействии сотрудников Банка не дожидаясь окончания монтажных работ на остальных объектах обеспечивают настройку оборудования. Задаются параметры работы исполнительного оборудования, вносится информация о полномочиях пользователей, проводится тестирование СКУД в различных условиях. Отдельным этапом проводится проверка работоспособности системы при срабатывании охранно-пожарной сигнализации.

2.5 Описание внедрения системы Lenel в филиалах Свердловского отделения № 7003 ПАО Сбербанк

2.5.1 Этап 1. Проектирование системы для дальнейшей реализации

На данном этапе были проанализированы существующие решения и технологии на каждом из филиалов. Проведено обследование объектов, дана оценка целесообразности, с учетом всех структурных изменений произошедших в банке, установки имеющихся исполнительных устройств. Спрогнозировано дальнейшее развитие проекта с учетом предстоящих изменений

в банке. Проанализирован рынок СКУД, имеющиеся у каждого производителя технические решения и возможность интеграции их оборудования с системами банка.

Необходимость интеграции с имеющейся системой СКУД легли в основу технического задания. Главной задачей стала оценка возможности распределенного функционирования системы при централизованном администрировании. Наличие на объектах заказчика помещений используемых территориальным банком определили требования к возможности разделения прав администрирования для каждого контроллера. Принципиальная сема работы создаваемой СКУД представлена на рисунке 17.

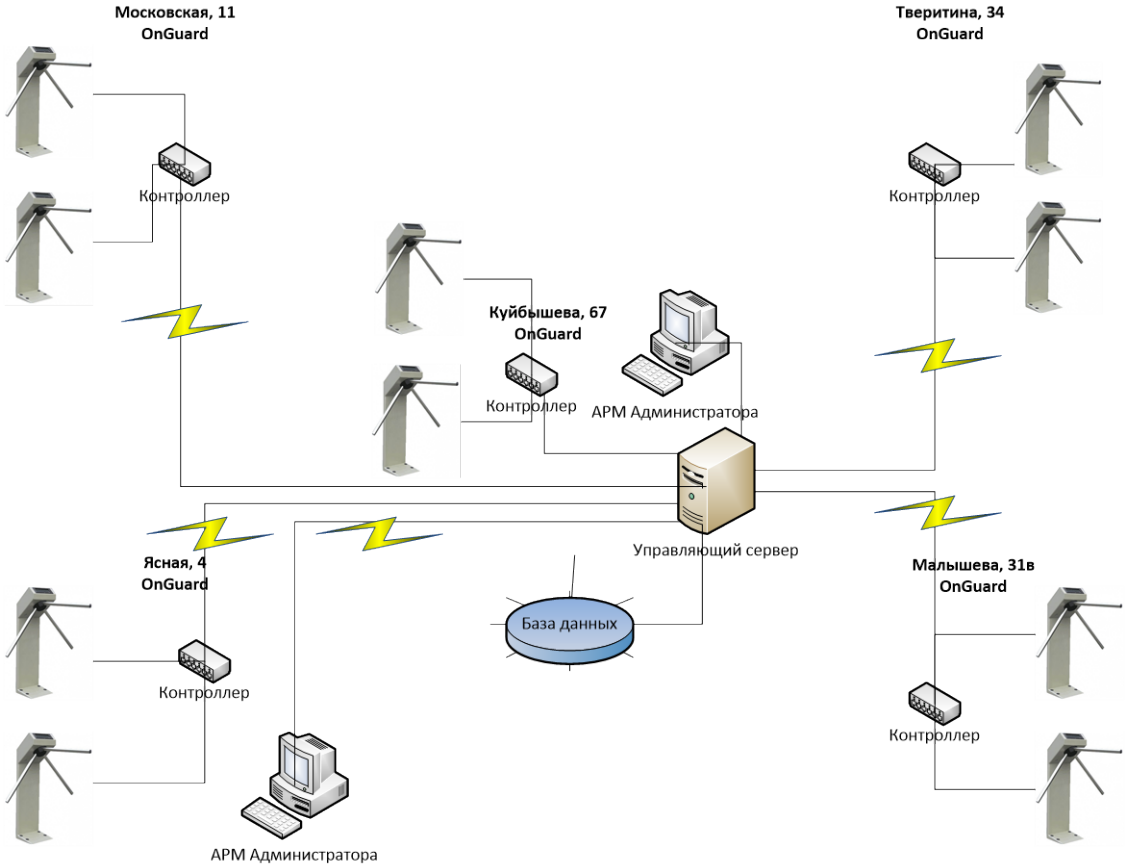

Рисунок 17 – Принципиальная схема работы создаваемой СКУД

На основе данных анализа конфигурации имеющегося оборудования ONGuard компании Lenel и обследования объектов сформулированы следующие требования, которые являются основой технического задания (Приложение 2):

1. Все устанавливаемое оборудование должно быть интегрировано в существующую систему контроля и управления доступом на базе оборудования марки Lenel административного здания Уральского банка ПАО Сбербанк расположенного по адресу: ул. Куйбышева, 67.

2. Смонтированное оборудование СКУД предназначено для непрерывной круглосуточной работы в режиме постоянной связи с сервером системы. При этом оно должно обеспечивать:

- максимальное число регистрируемых событий за одни сутки – не менее 100000;
- средняя плотность потока событий – не менее 10 событий в секунду (для каждого события обеспечить прием, обработку и регистрацию в журнале событий);
- пиковая плотность потока событий – не менее 100 событий в секунду (продолжительность пиковой нагрузки не более 10 минут, для каждого события обеспечить прием, обработку и регистрацию в журнале событий);
- максимальное количество карт доступа – не менее 75000;
- максимальное количество операторов системы (паролей) – не менее 50;
- максимальное количество одновременно работающих клиентских программ (АРМ) – не менее 32;
- максимальное количество одновременно работающих АРМ «Бюро пропусков» не менее 10;
- создание отчетов по конфигурации системы;
- создание отчетов по всем происшедшим событиям за любой интервал времени;
- разграничение прав доступа операторов к просмотру и изменению информации, конфигурированию и управлению модульными контроллерами;

- учет рабочего времени и фиксацию фактов опоздания сотрудников с составлением соответствующих отчетов (по суммарному времени за заданный период времени, по ежедневному отработанному времени, детальные отчеты по входу и выходу), при этом фильтры для задания отчетов должны содержать дату и время временных периодов отчетов, а также, такие поля из базы данных, как: номер структурного подразделения, функциональный блок, департамент, управление, отдел, фамилия, имя, отчество, должность, номер карточки;
- подготовка отчетов должна осуществляться как по любому отдельному из указанных параметров фильтра, так и по любой комбинации параметров. При создании отчетов должны применяться такие условия сравнения задаваемых параметров, как: начинается, содержит, равно, не равно, больше, меньше, и др.;
- отчеты по опозданиям должны учитывать транзакции сотрудников, вошедших в здание до заданного в фильтре времени начала отчета, с целью исключения попадания этих сотрудников в категорию опоздавших;
- все отчеты должны содержать по возможности корректные и достоверные данные вне зависимости от возможных сбоев при считывании карточек и нестандартных транзакций (например, два входа или выхода подряд, произошедших, в том числе, при переходе через сутки или более).;
- вывод отчетов в формате электронной таблицы MS EXCEL, в текстовом формате, в формате *.pdf;
- отображение фотографий всех лиц, идентифицирующихся на считывателях точек доступа входных групп объекта (как «на вход», так и «на выход»), на мониторах АРМ соответствующих постов охраны;
- наращивание и расширение системы без замены центрального оборудования и ПО;
- отображение информации о техническом состоянии оборудования, о происходящих системных событиях на графических планах охра-

няемого объекта. Состояния технических средств должны отображаться в виде условных графических знаков. Поступающие события должны заноситься в виде текстовых сообщений в список, причем каждый тип события должен иметь собственное уникальное цветовое оформление;

- подачу оператором произвольной заранее запрограммированной группы команд по отношению к устройствам;
- автоматическое выполнение заранее запрограммированных действий при выполнении определенных событий или условий;
- автоматическую проверку режима работы СКУД для выявления и коррекции ошибок передачи и приема сообщений, обнаружения отсутствия связи с контроллером и формирование соответствующих тревожны сообщений;
- создание отчетов по событиям технических средств;
- работу системы в компьютерной сети с созданием нескольких удаленных АРМ операторов постов охраны и АРМ администраторов;
- поддержку работы нескольких удаленных СКУД с общими базой данных пользователей, и базой событий в системах, расположенных на общем сервере с обеспечением автономной независимой работы этих удаленных СКУД в полном объеме, с автоматической синхронизацией баз данных и баз событий удаленных СКУД с общими базами данных (многофилиальный режим работы);
- санкционированный вход и выход в/из зоны ограниченного доступа после идентификации личности по БСК с любым форматом вещественных кодов, а так же, при необходимости, по биометрическим признакам;
- прием информации о событиях от контроллеров;
- отображение событий в СКУД на соответствующих автоматизированных рабочих местах (АРМ) в реальном времени в графическом и текстовом виде со звуковым сопровождением;

- выполнение команд операторов по отношению к модульным контроллерам;
- конфигурирование оборудования;
- долговременную регистрацию всех событий.

2.5.2 Этап 2. Подбор оборудования и составление сметы

Построение системы основывается на использовании различных компонентов. Будет приобретено программное обеспечение:

1. SWC-ADVI. Центральное программное обеспечение Lenel, для администрирования СКУД. Помимо непосредственного администрирования баз данных пользователей, установки правил прохода позволяет осуществлять, мониторинг событий, редактирование графических планов, интеграцию СКУД с CCTV, автоматическую отправку E-mail, видеоверификацию, патрулирование, ввод фото, экспорт фото, дизайн пропуска, печать пропуска.

2. SWG-1240, Лицензия «Сегментация» - разделение базы данных на сегменты. Программное обеспечение предоставляет возможность создания отдельных сегментов, каждый из которых может иметь свои уникальные параметры и принципы управления, такие как уровни доступа, часовые пояса, распределенные сценарии, пользователей и т.д. Администратор в системе может управлять индивидуальным, предоставленным только ему объектом. Главная задача программного обеспечения разделить администрирование управляемых устройств СКУД территориального банка и Свердловского отделения № 7003.

3. PRO-64RUP, Лицензия на дополнительные 64 считывателя для PRO сервера, Lenel.

Примерная номенклатура приобретаемого и имеющегося в наличии оборудования включает:

- NGP-1320-UMP Модуль управления 2-мя дверьми (с комплектом для установки в CTX). 2 двери (4 считывателя, вход/выход). 8 входов, 6 релейных выходов, 12/24VDC, 840mA, (RoHS, CE, UL294, C-Tick). Внешний вид представлен на рисунке 18;

Рисунок 18 – Модуль управления NGP-1320-UMP

- NGP-3320CE Контроллер (функционал СКУД), управление 2-мя дверьми (подкл. 4 считывателя), поддержка до 130 дверей (считыватели на вход/выход). До 96 дополнительных модулей, до 500.000 пользователей и 50.000 событий. 4 Порта SNAPP (RS-485, не более 24 модулей на порт). Два встроенных порта Ethernet (с резервной связью). В металлическом боксе, со встроенным источником питания 220VAC (RoHS, CE);
- NGP-2220CE Контроллер (функционал СКУД), управление 2-мя дверьми (подкл. 4 считывателя), поддержка до 66 дверей (считыватели на вход/выход). До 96 дополнительных модулей, до 250.000 пользователей и 50.000 событий. 4 Порта SNAPP (RS-485, не более 24 модулей на порт). Встроенный порт Ethernet. В металлическом боксе, со встроенным источником питания 220VAC (RoHS, CE). Внешний вид представлен на рисунке 19;

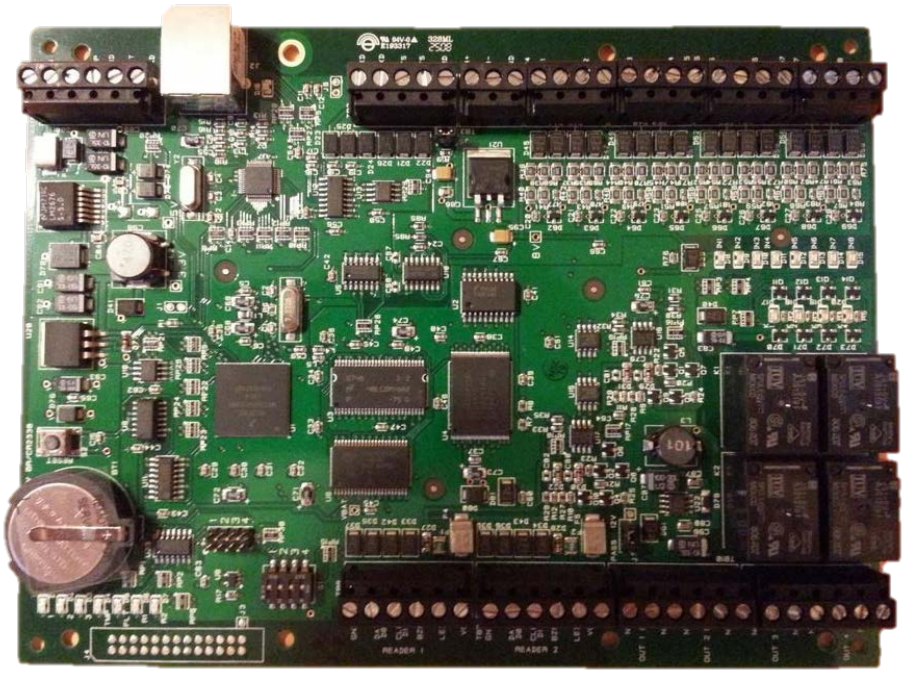

Рисунок 19 – Контроллер NGP-2220CE

- RWKLB575 iCLASS, бесконтактный считыватель Смарт карт с клавиатурой, LCD дисплеем, встроенным считывателем отпечатка пальца, поддерживающий чтение и запись данных , до 20 см, интерфейс Виганда, RS-232, RS-485, USB;
- R10 SE iCLASS Считыватель карт iClass, iClass SE, только чтение, интерфейс Wiegand, до 8.9 см, -40°- 65° C, 4.8 x 10.3 x 2.3 см, 5-16 В DC, 115 мА. Внешний вид представлен на рисунке 20;

Рисунок 20 – Считыватель карт iClass

- 6121BKT0000PRGL, Считыватель/программатор смарткарт iCLASS RW400 READ/WRITE Card Programmer. Специальная прошивка Lenel;
- MSO 300, Биометрический считыватель, интерфейс USB, размер сканера 22x24 мм (500 т/дюйм), Morpho. Внешний вид представлен на рисунке 21;

Рисунок 21 – Биометрический считыватель MSO 300

- Картоприемник PERCo-IC03.1;
- ST-EX010SM. Кнопка «ВЫХОД» металлическая, накладная, НР контакты, размер: 83x32x25 мм. Smartec;
- ST-DB510MT, Эл-мех. соленоидный замок, мониторинг, НО, питание 12VDC / 150мА (пик 900мА), цельнометаллический ригель, сила удержания 1000кг, Smartec (для пом. 403, 404);
- ST-EL250ML, Электромагнитный замок, мониторинг, СИД, внутреннее исполнение, 12 VDC / 500мА или 24VDC / 250мА, усилие 250 кг., Smartec. Внешний вид представлен на рисунке 22;

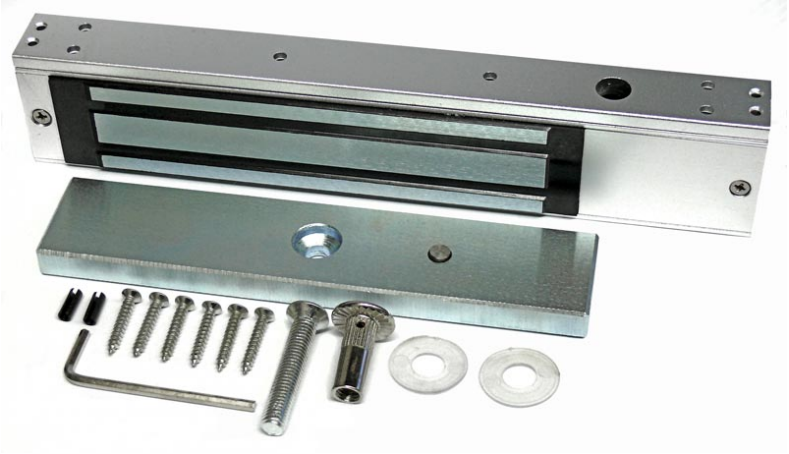

Рисунок 22 – Электромагнитный замок

- ST-BR250LC, L-образное крепление с крышкой возможностью регулировки для замка ST-EL250ML, Smartec. Внешний вид представлен на рисунке 22;

Рисунок 23 – L-образное крепление

- 2002 HID Бесконтактная смарт-карта iCLASS, память 16 Кб, 16 секторов, тонкая - для печати на принтере, 5.40x8.57x0.084 см.;
- ST-BX001, Металлический бокс, установка максимум 2 плат. Габариты: 30x40x11 см, Smartec;
- ST-PS105C, Б.б.п. 12 VDC/ 5 A; 220 VAC; корпус 195x265x75 мм (место для аккумулятора 10 Ач), Smartec;
- Замок электромагнитный/электромеханический;
- Турникет. Внешний вид представлен на рисунке 24.

Рисунок 24 – Турникет

Все компоненты СКУД будут подключены к локальной сети передачи данных заказчика. При этом для соблюдения требований информационной безопасности выделен отдельный сегмент сети, предоставлен пул IP адресов.

Дополнительных требований к скорости передачи данных не предъявляется, используется стандартная скорость 128 kb/s.

Проектная группа подрядной организации готовит проектную документацию, согласованные монтажные бригады осуществляют монтаж оборудования по графику, который готовится до начала работ, и является контрольным документом соблюдения сроков проведения работ.

2.5.3 Этап 3. Монтаж и настройка оборудования

После заключения договора, в связи с наличием у заказчика регламента допуска представителей (работников) сторонних организаций, подрядной организацией готовится список специалистов участвующих в монтаже оборудования. Все лица проходят согласование со службой безопасности, при наличии фактов невозможности допуска на объекты в перечень лиц вносятся корректировки.

На первоначальном этапе устанавливается исполнительное оборудование, проводятся интерфейсные коммуникации до контроллеров. Принципиальным требованием обеспечения отказоустойчивости системы является прямое соединение контроллеров с ближайшим сетевым маршрутизатором, от которого обеспечивается прямая связь с сервером СКУД.

Для помещений с ограниченным доступом подключаются биометрические считыватели.

Параллельно с установкой оборудования производится настройка программного обеспечения, разграничиваются права доступа управления замками, вносятся необходимые данные о зонировании помещений в соответствии с имеющимися в банке требованиями.

Для пользователей определяются права доступа и вносятся соответствующие ограничения администратором системы, при необходимости вносятся данные о привязке идентификатора, производится печать фотографии сотрудника. Отдельная категория сотрудников, имеющая доступ в режимные помещения, предоставляет биометрические сведения, которые связываются с карточкой пользователя.

Проводятся тестовые испытания.

2.5.4 Этап 4. Тестирование и обслуживание

После настройки и тестирования СКУД отделом охраны управления безопасности Свердловского отделения будет организована выдача электронных идентификаторов пользователям.

Каждый пользователь будет проинструктирован о порядке использования электронных идентификаторов. Доведены требования пропускного режима, порядка формирования заявок на изготовление новых идентификаторов и внесения изменений в существующие зоны доступа.

Учитывая последовательный процесс монтажа и ввода СКУД, изготовление и выдача электронных идентификаторов будут осуществлены для сотрудников работающих на соответствующих объектах, при этом единая база данных пользователей позволит, вторым этапом, организовать выдачу карт для остальных сотрудников не дожидаясь окончания монтажа.

Основными рисками на данном этапе являются:

- предоставление сотрудникам несоответствующего должностным обязанностям права доступа;
- ошибки соответствия электронных идентификаторов пользователям;
- общий отказ системы;
- невозможность доступа в режимные помещения из-за неверно введённых биометрических данных

- саботирование сотрудниками требований безопасности.

Сотрудниками отделов охраны и технических средств охраны управления безопасности для минимизации последствий при возможности реализации указанных рисков будут проведены предупреждающие мероприятия:

- обеспечен двойной контроль прав пользователей;
- разработаны методические рекомендации;
- назначены ответственные сотрудники за мониторинг состояния СКУД;
- проведены инструктажи сотрудников;
- внесенные изменения в регламенты утверждены руководством.

Одним из важных этапов внедрения СКУД является обучение пользователей работе с СКУД. Специалисты подрядной организации предоставляют лекционный материал и проводят практические занятия с работниками заказчика, специально назначенными для администрирования СКУД. В рамках этапа работники получаю знания по конфигурации оборудования, техническим характеристикам, возможностям настройки системы. Практические занятия предоставляют возможность отработать действия по настройки и эксплуатации системы.

3 ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА И ПРИМЕРНАЯ СМЕТА ВНЕДРЕНИЯ

Эксплуатируемые, в банке, СКУД обеспечивают необходимый уровень режимности. Наличие различных зон доступа, необходимость обеспечения сохранности денежных средств, дорогостоящего имущества и информации обуславливает потребность создавать системы безопасности и нести операционные расходы на их содержание. Устарелость СКУД, территориальное распределение объектов определяют уровень дополнительных расходов.

Стоимость риска, связанную с выходом выработавших ресурс СКУД, в связи с отсутствием запасных частей можно рассчитать, приравняв сломанный компонент к стоимости поста физической охраны.

Не маловажным не ценовым фактором является минимизация риска компрометации электронных идентификаторов у сотрудников, не имеющих права на вход в банка, таких как:

- уволенные;
- находящиеся в декретном отпуске;
- находящиеся отпуске по уходу за ребенком;
- находящиеся в очередном отпуске;
- временно не трудоспособные.

Еще одним не ценовым фактором является лояльность сотрудников банка к сервису изготовления электронных идентификаторов. До внедрения централизованной СКУД вновь принятому сотруднику банка приходится ожидать не менее одной недели до получения готового электронного идентификатора.

Расчет единовременных капитальных затрат

Суммарные затраты на реализацию проекта $C_{реал}$ включают в себя:

$C_{реал} = C_{оборуд} + C_{монтаж}$ (1.1)

Следует отметить, что стоимость разработки проектной документации, по условиям договора, в расходы подрядчика и учитывается в стоимости монтажных и пусконаладочных работ.

Для расчета стоимости оборудования $С_{оборуд}$ внесем информацию о розничной цене в таблицу 5.

Таблица 5 – Розничная стоимость оборудования

Наименование оборудования, материалов и работ, выполняемых Подрядчиком	**Ед.**	**Кол-во**	**Стоимость с НДС за ед., руб.**	**Сумма с НДС, руб.**
1	2	3	4	5
SWC-ADVI, ПО - клиент ADVI. Включает администрирование, мониторинг, редактор графических планов, интеграцию с CCTV, автоматическую отправку E-mail, видеоверификацию, патрулирование, ввод фото, экспорт фото, дизайн пропуска, печать пропускаа, Lenel.	шт.	1	989 209,17	989 209,17
SWG-1240, Лицензия «Сегментация» - разделение базы данных на сегменты, только для ADV и PRO.	шт.	1	764 560,55	764 560,55
PRO-64RUP, Лицензия на дополнительные 64 считывателя для PRO сервера, Lenel.	шт.	4	407 170,01	1 628 680,04
NGP-3320CE Контроллер (функционал СКУД), управление 2-мя дверьми (подкл. 4 считывателя), поддержка до 130 дверей (считыватели на вход/выход). До 96 дополнительных модулей, до 500.000 пользователей и 50.000 событий. 4 Порта SNAPP (RS-485, не более 24 модулей на порт). Два встроенных порта Ethernet (с резервной связью). В металлическом боксе, со встроенным источником питания 220VAC (RoHS, CE).	шт.	2	292 433,68	584 867,36
NGP-2220CE Контроллер (функционал СКУД), управление 2-мя дверьми (подкл. 4 считывателя), поддержка до 66 дверей (считыватели на вход/выход). До 96 дополнительных модулей, до 250.000 пользователей и 50.000 событий. 4 Порта SNAPP (RS-485, не более 24 модулей на порт). Встроенный порт Ethernet. В металлическом боксе, со встроенным источником питания 220VAC (RoHS, CE)., Lenel.	шт.	2	279 140,40	558 280,80

Продолжение таблицы 5

NGP-1320-UMP Модуль управления 2-мя дверьми (с комплектом для установки в CTX). 2 двери (4 считывателя, вход/выход). 8 входов, 6 релейных выходов, 12/24VDC, 840mA, (RoHS, CE, UL294, C-Tick).	шт.	74	80 983,21	5 992 757,54
6121BKT0000PRGL, Считыватель/программатор смарткарт iCLASS RW400 READ/WRITE Card Programmer. Специальная прошивка Lenel.	шт.	2	43 274,00	86 548,00
Evolis PM1H0VVCxS односторонний принтер пластиковых карт для цветной печати с кодировщиком контактных карт HID iClass и бесконтактных карт Mifare, USB & Ethernet.	шт.	1	175 123,00	175 123,00
MSO 300, Биометрический считыватель, интерфейс USB, размер сканера 22x24 мм (500 т/дюйм), Morpho.	шт.	2	40 040,00	80 080,00
R10 SE iCLASS Считыватель карт iClass, iClass SE, только чтение, интерфейс Wiegand, до 8.9 см, -40°- 65° C, 4.8 x 10.3 x 2.3 см, 5-16 В DC, 115 мА.	шт.	159	10 087,00	1 603 833,00
RWKLB575 iCLASS, бесконтактный считыватель Смарт карт с клавиатурой, LCD дисплеем, встроенным считывателем отпечатка пальца, поддерживающий чтение и запись данных , до 20 см, интерфейс Виганда, RS-232, RS-485, USB.	шт.	8	73 150,00	585 200,00
Картоприемник PERCo-IC03.1.	шт.	3	68 880,00	206 640,00
ST-EL250ML, Электромагнитный замок, мониторинг, СИД, внутреннее исполнение, 12 VDC / 500мА или 24VDC / 250мА, усилие 250 кг., Smartec.	шт.	2	2 849,00	5 698,00
ST-BR250LC, L-образное крепление с крышкой возможностью регулировки для замка ST-EL250ML, Smartec.	шт.	2	1 386,00	2 772,00
ST-DB510MT, Эл-мех. соленоидный замок, мониторинг, НО, питание 12VDC / 150мА (пик 900мА), цельнометаллический ригель, сила удержания 1000кг, Smartec (для пом. 403, 404).	шт.	2	4 235,00	8 470,00
ST-EX010SM. Кнопка «ВЫХОД» металлическая, накладная, НР контакты, размер: 83x32x25 мм. Smartec.	шт.	96	693,00	66 528,00
ST-BX001, Металлический бокс, установка максимум 2 плат. Габариты: 30x40x11 см, Smartec.	шт.	39	5 580,96	217 657,44

Окончание таблицы 5

ST-PS105C, Б.б.п. 12 VDC/ 5 А; 220 VAC; корпус 195х265х75 мм (место для аккумулятора 10 Ач), Smartec.	шт.	18	4 312,00	77 616,00
ST-PS110E, Б.б.п. 12 VDC/ 10 А; 220 VAC; корпус 285х395х165 мм (место для 2-х аккумуляторов 17 Ач), Smartec.	шт.	9	9 625,00	86 625,00
ST-BT110, Аккумулятор 12 В, 10 Ач, 151х65х111 мм, Smartec.	шт.	18	1 925,00	34 650,00
ST-BT117, Аккумулятор 12 В, 17 Ач, 180х77х168 мм, Smartec.	шт.	18	3 080,00	55 440,00
2002 HID Бесконтактная смарт-карта iCLASS, память 16 Кб, 16 секторов, тонкая - для печати на принтере, 5.40х8.57х0.084 см.	шт.	1000	620,62	620 620,00
Картридж YMCKO 200/ Лента для полноцветной печати YMCKO, 200 карт (для Evolis Zenius).	шт.	5	5 395,00	26 975,00
Коробка соединительная с клеммниками.	м.	128	185,00	23 680,00
КСПВ 4х0,5 Кабель слаботочный.	м.	8695	6,63	57 647,85
ШВВП 2х0,75 Шнур питания.	м.	8695	12,48	108 513,60
ВВГнг-LS 3х2,5.	м.	820	46,28	37 949,60
UTP 4х2х0,52 Кабель «витая пара».	м.	9235	21,25	196 243,75
14 882 865,70				

Стоимость монтажных работ условиями договора определена как 18% стоимости монтажа. Таким образом, $C_{монтаж}$ = 2 678 915,83 руб.

Стоимость пусконаладочных работ по условиям договора составляет 4% и равна $C_{пуск}$ = 595 314,63 руб.

Согласно (1.1.) получим, что стоимость реализации проекта равна:

$C_{реал}$ = 14 882 865,70+ 2 678 915,83 + 595 314,63 = 18 157 096,16 руб.

Расчет текущих затрат до внедрения проекта

Эксплуатационными затратами на администрирование СКУД является заработная плата двух сотрудников отдела технических средств охраны.

Оклад составляет 34000 рублей и 29090 руб.

Уральский коэффициент (15%) – 5100 рублей и 4363,50 руб. соответственно.

Действующая в банке система мотивации предусматривает для данной категории сотрудников 50% квартальное премирование и 100% годовое премирование. Таким образом, премиальная оплата труда – 17000 руб. и 14545 руб. в квартал и 34000 руб. и 29090 руб. в год.

Итого годовой ФОТ составляет (34000+5100+29090+4363,50)·12 + + (17000 +14545)·4+34000+29090 = 1059912 руб.

Отчисления в социальные фонды на двух работников (30,2%) – 320093,42 руб. в год.

Таким образом, годовые текущие затраты до внедрения проекта составляют:

1059912 + 320093,42 = 1380005,42 руб.

Стоимость транспортного обеспечения

С Ясной, 4 на каждый объект в течение недели 2 раза осуществляется выезд специалистов.

Расстояние до объектов:

Московская, 11 – 3,56 километра;

Тверитина, 34 – 3,44 километра;

Малышева, 31в – 4,15 километра.

Средняя стоимость одного километра пути при использовании автотранспорта – 17,5 рублей. Количество недель в году – 52.

Стоимость транспортного обеспечения в год будет составлять:

$С_{трансп} = (3,56 + 3,44 + 4,15) \cdot 2 \cdot 17,5 \cdot 52 = 20293$ руб. в год.

Стоимость альтернативных методов обеспечения уровня безопасности

Для обеспечения аналогичного уровня, сопоставимого с эксплуатацией устанавливаемого СКУД необходимо привлечение 5 суточных и 21-14 часовых поста физической охраны. При средней стоимости предоставления услуг 120 руб. в час, расходы будут составлять:

$C_{охран} = (5 \cdot 24 + 21 \cdot 14) \cdot 365 \cdot 120 = 18133200$ руб.

Расчет текущих затрат после внедрения проекта

После реализации проекта, администрированием СКУД будет заниматься один специалист. Стоимость экономии одного специалиста (34000+5100)·12 + 17000·4 + 34000 = 571200 руб. в год

Возможность удаленного администрирования позволить исключить потребность транспортных расходов, стоимость которых равна 20293 руб. в год.

Внедрение СКУД позволит сократить 1 суточный и 1 полусуточный посты физической охраны. Экономия составит $(1 \cdot 24 + 1 \cdot 12) \cdot 365 \cdot 120 = 1576800$ руб. в год.

Автоматизация учета рабочего времени

Интеграция СКУД с автоматизированной системой учета рабочего времени позволит сократить расходы на ведение табеля.

В соответствии с требованиями банка в каждом подразделении назначается ответственный специалист (старший специалист), со средним окладом 30090 рублей, в обязанности которого входит ежедневное заведение сведений о выходе работников и фактически отработанного ими времени.

Для ввода сведений в систему, на каждого сотрудника тратиться 1 минута рабочего времени ежедневно.

Применение правила учета будет возможно для 1679 сотрудников. Таким образом, автоматизация процесса позволит сократить 1679 минут в день. В соответствии с производственным календарем в 2016 году 247 рабочих дней, временные затраты при ручном методе ввода составят $247 \cdot 1679 = 414713$ минут, или 6911,88 часа.

Стоимость одного часа рабочего времени табельщика составляет:

$$C_{таб} = \left(\frac{Оклад \cdot 12}{норма\ часов\ в\ год}\right) = \frac{30090 \cdot 12}{1974} = 182{,}92 \text{ руб./час.}$$

Автоматизация учета рабочего времени позволит сократить расходы банка на $6911{,}88 \cdot 182{,}92 = 1264321{,}08$ руб.

Эффективность внедрения

СКУД с учетом статуса заказчика базовая функция, необходимая для поддержания соответствующего уровня защищенности. Банк вынужден нести расходы на содержание и поддержание её в работоспособном состоянии.

Приведенные расчеты показали, что внедрение современной системы дорогостоящий проект, но при этом возможно достичь снижения операционных расходов за счет централизации администрирования, а также внедрения СКУД в автоматизированные процессы.

ЗАКЛЮЧЕНИЕ

Обеспечение высокого уровня безопасности всех производственных процессов – важная задача для функционирования банка. Несанкционированные проходы, нарушения пропускного режима и трудовой дисциплины, нецелевое использование рабочего времени – все это несет потенциальную угрозу, способную привести к существенным материальным издержкам.

Для обеспечения контроля доступа в банке необходимо внедрение современной СКУД, в состав которой будут входить различные средства для аутентификации (считыватели карт, биометрические считыватели и идентификаторы), контроллеры и исполнительные устройства (турникеты, ворота и т. д.). Каждому работнику определяется уровень доступа, выдаются персональные идентификаторы, с помощью которых они могут проходить на территорию банка и в помещения, где имеют право находиться.

Реализация мероприятий по внедрению СКУД начата в первом квартале 2016 года. На текущий момент, в соответствии с планом разработан проект и осуществляется выбор подрядной организации. Согласованная, территориальным банком, документация рассмотрена на заседании конкурсной комиссии.

Мероприятия по монтажу оборудования и его настройке, администрированию системы запланированы на 3 квартал 2016 года. Ввод в эксплуатацию будет осуществляться поэтапно начиная с 3 квартала и должен быть завершен до конца 2016 года.

Таким образом, задачи решены, цели достигнуты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Веб-системы контроля доступа [Электронный ресурс]. – Режим доступа: http://www.security.honeywell.com/ru/products/access/so/ 779994.html/ (дата обращения: 16.05.2016).

2. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом. СПб.: Университет ИТМО, 2015. 53 с.

3. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия Телеком, 2015. 272с.

4. ГОСТ Р 54831-2011 «Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний» (утв. и введен в действие Приказом Росстандарта от 13.12.2011 N 1223-ст).

5. Гражданский кодекс Российской Федерации.

6. Джхунян В.Л., Шаньгин В.Ф. Электронная идентификация. М.: АСТ, НТ Пресс 2014. 696с.

7. Интегрированная система охраны «Орион» [Электронный ресурс]. – Режим доступа: http://bolid.ru/production/orion/po-orion/arm_orion_pro.html (дата обращения: 16.05.2016).

8. Информация о Банке [Электронный ресурс]. – Режим доступа: http://www.sberbank.ru/ru/about/today/ (дата обращения: 16.05.2016).

9. Информация по кредитным организациям [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/credit/coinfo.asp?id =350000004/ (дата обращения: 20.05.2016).

10. Кашкаров А.П. Системы безопасности и устройства кодового доступа. Просто о сложном. М.: ДМК Пресс, 2014. 109 с.

11. Масштабируемые системы контроля доступа и интегрированные системы безопасности Lenel OnGuard [Электронный ресурс]. – Режим досту-

па: http://www.lenel.ru/news/access-control-system.ahtm/ (дата обращения: 16.05.2016).

12. Министерство по управлению государственным имуществом Свердловской области [Электронный ресурс]. – Режим доступа: http://mugiso.midural.ru/region/okn/estateekt.php?ELEMENT_ID=949/ (дата обращения: 19.05.2016).

13. Многофункциональный центр предоставления государственных и муниципальных услуг [Электронный ресурс]. – Режим доступа: http://www.mfc66.ru/news/8228/?sphrase_id=57566/ (дата обращения: 19.05.2016).

14. Не типичные функции СКУД [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/articles2/sys_ogr_dost/netipichnye-funktsii-skud/ (дата обращения: 20.05.2016).

15. Обзор возможностей СКУД [Электронный ресурс]. – Режим доступа: http://www.sistema-dostupa.ru/i03.htm/ (дата обращения: 16.05.2016).

16. Программно-аппаратный комплекс «Менуэт 2000». Руководство по эксплуатации. М.: Москва, 1999. 118 с.

17. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. СПб.: НИУИТМО, 2012. 157с.

18. Система контроля доступа на предприятии. Особенности внедрения [Электронный ресурс]. – Режим доступа: http://www.cleper.ru/articles/description.php?n=441 (дата обращения: 20.05.2016).

19. Система контроля и управления доступом. Принцип действия [Электронный ресурс]. – Режим доступа: http://www.intersyst.ru/solutions/165/460/ (дата обращения: 14.05.2016).

20. Сорокин К. Применение биометрических технологий в обеспечении информационной безопасности бизнеса. //СКУД. Антитеррористм-2013 2013 С. 46-47.

21. Тихонов О.О., Малышева А.С., Шаповалов А.В., Гамбург А.Е., Стасенко Л.А, Курилин А.С. Функции универсальных СКУД: что нужно потребителю. //Системы безопасности 2011 № 4. С. 108-119.

22. Федеральный закон от 05.04.2013 N 44-ФЗ (ред. от 02.06.2016) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

23. Федеральный закон от 18.07.2011 N 223-ФЗ (ред. от 13.07.2015) «О закупках товаров, работ, услуг отдельными видами юридических лиц».

24. Федеральный закон от 26.07.2006 N 135-ФЗ (ред. от 05.10.2015) «О защите конкуренции» (с изм. и доп., вступ. в силу с 10.01.2016).

25. Шабалин А. Обзор Российского рынка СКУД. //ДИРЕКТОР ПО БЕЗОПАСНОСТИ 2014 № 7. С. 36-42.

ПРИЛОЖЕНИЕ 1

Министерство образования и науки Российской Федерации

ФГАОУ ВО «Российский государственный

профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
Направление подготовки 09.03.03 Прикладная информатика
Профиль подготовки «Прикладная информатика в экономике»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Н.С. Толстова
подпись фамилия и. о.

«____» _____ 2016г.

ЗАДАНИЕ
на выполнение квалификационной работы бакалавра

студента (ки) 5 курса группы КП-511-ИЭ
Вахрушева Андрея Сергеевича
фамилия, имя, отчество полностью

1. Тема Внедрение системы контроля доступом в Свердловском отделении Сбербанка

утверждена распоряжением по институту от «__» _____ 2016г. № ___

2. Руководитель Ченушкина Светлана Владимировна
фамилия, имя, отчество полностью

_____ _____ ст.преподаватель каф. ИС РГППУ
ученая степень ученое звание должность место работы

3. Место практики ПАО Сбербанк

4. Исходные данные к ВКР
1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом.
2. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом.
3. Джхунян В.Л., Шаньгин В.Ф. Электронная идентификация.
4. Рыжова В.А. Проектирование и исследование комплексных систем безопасности

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
1. Рассмотрение основных возможностей систем контроля доступа и провести анализ возможностей существующих систем
2. Анализ существующего состояния пропускных систем на различных объектах предприятия заказчика

3. Выбор и обоснование методологии внедрения системы на предприятии

4. Оценка экономической эффективности программного обеспечения .

5. Расчет экономического обоснования проекта и примерной сметы внедрения

6. Перечень демонстрационных материалов

Графическая часть представлена презентацией в MS Power Point.

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполне-ния ВКР	Отметка руководителя о выполнении
1	Сбор информации по работе и сдача зачета по практике		15	
2	Выполнение работ по разрабатываемым вопросам их изложение в работе: Анализ предметной области Разработка программного обеспечения Расчет экономической эффективности программы		50	
3	Оформление текстовой части ВКР		15	
4	Выполнение демонстрационных материалов к ВКР		5	
5	Нормоконтроль		10	
6	Подготовка доклада к защите в ГЭК		5	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата
		подпись	дата	подпись	дата
		подпись	дата	подпись	дата

Руководитель _____ _____ *Задание получил* _____ _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить Вахрушева А.С. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Вахрушева А.С. к защите выпускной квалификационной работы
фамилия и. о. студента

в государственной экзаменационной комиссии (протокол заседания кафедры от «___» _____ 2016г., № _____)

Заведующий кафедрой _____ _____
подпись дата

ПРИЛОЖЕНИЕ 2

Техническое задание
на создание системы контроля и управления доступом (СКУД)

на Объектах Заказчика, по адресам, указанным в Приложениях №1А,1Б, 1В, 1Г к Договору

Создание систем безопасности - системы контроля и управления доступом (СКУД) ДО № 7003/0504 Свердловского отделения № 7003 ПАО Сбербанк, г. Екатеринбург, ул. Московская, 11; ДО № 7003/0503 Свердловского отделения № 7003 ПАО Сбербанк, г. Екатеринбург, ул. Малышева, 31 В; ДО № 7003/0501 Свердловского отделения № 7003 ПАО Сбербанк, г. Екатеринбург, ул. Тверитина, 34; ДО № 7003/0448 Свердловского отделения № 7003 ПАО Сбербанк, г. Екатеринбург, ул. Ясная, 4.

1. Под созданием электронной системы безопасности понимается выполнение Подрядчиком совокупности работ по оборудованию помещений банка системой контроля и управлением доступом, с целью оптимизации процесса получения ключей сотрудниками Банка от служебных помещений, а так же для получения информации о времени вскрытия/закрытия служебного помещения, сотруднике Банка производящего вскрытие/закрытие. В целях исключения ведения «Книги приема и сдачи ключей и служебных помещений» на бумажном носителе. В рамках выполняемых работ Подрядчик производит поставку оборудования, его установку на соответствующие помещения Объекта, а так же пуско-наладку и программирование установленного оборудования.

2. Сроки (периоды) выполнения работ: Поставка оборудования осуществляется в течение 90 (девяносто) календарных дней с даты подписания договора последней Стороной. Монтаж, пуско-наладка и программирование оборудования осуществляется в течение 90 (девяносто) календарных дней с даты передачи Подрядчику оборудования в монтаж.

3. Место выполнения работ: ДО № 7003/0504 Свердловского отделения № 7003 ПАО Сбербанк, расположенный по адресу: г. Екатеринбург, ул. Московская, 11; ДО № 7003/0503 Свердловского отделения № 7003 ПАО Сбербанк, расположенный по адресу: г. Екатеринбург, ул. Малышева, 31 В; ДО № 7003/0501 Свердловского отделения № 7003 ПАО Сбербанк, расположенный по адресу: г. Екатеринбург, ул. Тверитина, 34; ДО № 7003/0448 Свердловского отделения № 7003 ПАО Сбербанк, расположенный по адресу: г. Екатеринбург, ул. Ясная, 4.

4. Требования к качеству работ, и иные показатели, связанные с определением соответствия работ, оборудования потребностям Заказчика или целям их использования:

4.1.Все устанавливаемое оборудование должно быть интегрировано в существующую систему контроля и управления доступом административного здания Уральского банка ПАО Сбербанк расположенного по адресу: ул. Куйбышева, 67, установленную в соответствии с Проектом 2007.42-СБ.1 «Системы контроля и управления доступом и охранного телевидения» - 2 тома и Исполнительной документацией ИД-СБ.3 «Система контроля и управления доступом» - 5 томов, на базе оборудования марки Lenel.

4.2.Все оборудование должно иметь сертификаты соответствия Российских Федеральных центров сертификации, аккредитованных Госстандартом России или другую документацию.

4.3.Смонтированное оборудование СКУД предназначено для непрерывной круглосуточной работы в режиме постоянной связи с сервером системы. При этом должно обеспечивать:

- максимальное число регистрируемых событий за одни сутки – не менее 100000;
- средняя плотность потока событий – не менее 10 событий в секунду (для каждого события обеспечить прием, обработку и регистрацию в журнале событий);

- пиковая плотность потока событий – не менее 100 событий в секунду (продолжительность пиковой нагрузки не более 10 минут, для каждого события обеспечить прием, обработку и регистрацию в журнале событий);
- максимальное количество карт доступа – не менее 75000;
- максимальное количество операторов системы (паролей) – не менее 50;
- максимальное количество одновременно работающих клиентских программ (АРМ) – не менее 32;
- максимальное количество одновременно работающих АРМ «Бюро пропусков» не менее 10.
- создание отчетов по конфигурации системы;
- создание отчетов по всем происшедшим событиям за любой интервал времени;
- разграничение прав доступа операторов к просмотру и изменению информации, конфигурированию и управлению модульными контроллерами;
- учет рабочего времени и фиксацию фактов опоздания сотрудников с составлением соответствующих отчетов (по суммарному времени за заданный период времени, по ежедневному отработанному времени, детальные отчеты по входу и выходу), при этом фильтры для задания отчетов должны содержать дату и время временных периодов отчетов, а также, такие поля из базы данных, как: номер структурного подразделения, функциональный блок, департамент, управление, отдел, фамилия, имя, отчество, должность, номер карточки;
- подготовка отчетов должна осуществляться как по любому отдельному из указанных параметров фильтра, так и по любой комбинации параметров. При создании отчетов должны применяться такие условия сравнения задаваемых параметров, как: начинается, содержит, равно, не равно, больше, меньше, и др.;

- отчеты по опозданиям должны учитывать транзакции сотрудников, вошедших в здание до заданного в фильтре времени начала отчета, с целью исключения попадания этих сотрудников в категорию опоздавших;
- все отчеты должны содержать по возможности корректные и достоверные данные вне зависимости от возможных сбоев при считывании карточек и нестандартных транзакций (например, два входа или выхода подряд, произошедших, в том числе, при переходе через сутки или более);
- вывод отчетов в формате электронной таблицы MS EXCEL, в текстовом формате, в формате *.pdf;
- отображение фотографий всех лиц, идентифицирующихся на считывателях точек доступа входных групп объекта (как «на вход», так и «на выход»), на мониторах АРМ соответствующих постов охраны;
- наращивание и расширение системы без замены центрального оборудования и ПО;
- отображение информации о техническом состоянии оборудования, о происходящих системных событиях на графических планах охраняемого объекта. Состояния технических средств должны отображаться в виде условных графических знаков. Поступающие события должны заноситься в виде текстовых сообщений в список, причем каждый тип события должен иметь собственное уникальное цветовое оформление;
- подачу оператором произвольной заранее запрограммированной группы команд по отношению к устройствам;
- автоматическое выполнение заранее запрограммированных действий при выполнении определенных событий или условий;
- автоматическую проверку режима работы СКУД для выявления и коррекции ошибок передачи и приема сообщений, обнаружения отсутствия связи с контроллером и формирование соответствующих тревожны сообщений;
- создание отчетов по событиям технических средств;

- работу системы в компьютерной сети с созданием нескольких удаленных АРМ операторов постов охраны и АРМ администраторов;
- поддержку работы нескольких удаленных СКУД с общими базой данных пользователей, и базой событий в системах, расположенных на общем сервере с обеспечением автономной независимой работы этих удаленных СКУД в полном объеме, с автоматической синхронизацией баз данных и баз событий удаленных СКУД с общими базами данных (многофилиальный режим работы);
- санкционированный вход и выход в/из зоны ограниченного доступа после идентификации личности по БСК с любым форматом вещественных кодов, а так же, при необходимости, по биометрическим признакам;
- прием информации о событиях от контроллеров;
- отображение событий в СКУД на соответствующих автоматизированных рабочих местах (АРМ) в реальном времени в графическом и текстовом виде со звуковым сопровождением;
- выполнение команд операторов по отношению к модульным контроллерам;
- конфигурирование оборудования;
- долговременную регистрацию всех событий;
- Требования к безопасности выполняемых работ: Подрядчик обязан соблюдать требования по технике безопасности, охране труда, противопожарных, санитарных и иных правил, обеспечивающих безопасность выполняемых работ по Договору.