Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ЮРГИНСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ**
Федерального государственного автономного образовательного учреждения
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт: Юргинский технологический институт
Направление подготовки: 20.03.01 «Техносферная безопасность»
Профиль: «Защита в чрезвычайных ситуациях»

БАКАЛАВРСКАЯ РАБОТА

Тема работы
Проектирование СКУД на объекте банковской сферы

УДК 004.072.4:336.71

Студент

Группа	**ФИО**	**Подпись**	**Дата**
З-17Г51	Ширяева Ольга Сергеевна		

Руководитель/ консультант

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент ЮТИ ТПУ/ Ст. преподаватель ЮТИ ТПУ	Мальчик А.Г./ Деменкова Л.Г.	к.т.н./ -		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент ЮТИ ТПУ	Лизунков В.Г.	к.пед.н., доцент		

По разделу «Социальная ответственность»

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Доцент ЮТИ ТПУ	Солодский С.А.	к.т.н.		

Нормоконтроль

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Ст. преподаватель ЮТИ ТПУ	Деменкова Л.Г.	-		

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
ООП 20.03.01 «Техносферная безопасность»	Солодский С.А.	к.т.н.		

Юрга – 2020 г.

Планируемые результаты обучения по основной образовательной программе направления 20.03.01 – «Техносферная безопасность»

Код результатов	**Результат обучения (выпускник должен быть готов)**
Р1	Применять базовые и специальные естественнонаучные и математические знания, достаточные для комплексной инженерной деятельности в области техносферной безопасности.
Р2	Применять базовые и специальные знания в области техносферной безопасности для решения инженерных задач.
Р3	Ставить и решать задачи комплексного анализа, связанные с организацией защиты человека и природной среды от опасностей техногенного и природного характера, с использованием базовых и специальных знаний, современных аналитических методов и моделей, осуществлять надзорные и контрольные функции в сфере техносферной безопасности.
Р4	Проводить теоретические и экспериментальные исследования, включающие поиск и изучение необходимой научно-технической информации, математическое моделирование, проведение эксперимента, анализ и интерпретацию полученных данных, на этой основе разрабатывать технику и технологии защиты человека и природной среды от опасностей техногенного и природного характера в соответствии с техническим заданием и с использованием средств автоматизации проектирования.
Р5	Использовать знание организационных основ безопасности различных производственных процессов, знания по охране труда и охране окружающей среды для успешного решения задач обеспечения техносферной безопасности.
Р6	Обоснованно выбирать, внедрять, монтировать, эксплуатировать и обслуживать современные системы и методы защиты человека и природной среды от опасностей, обеспечивать их высокую эффективность, соблюдать правила охраны здоровья, безопасности труда, выполнять требования по защите окружающей среды.
	Универсальные компетенции
Р7	Использовать базовые и специальные знания в области проектного менеджмента для ведения комплексной инженерной деятельности.
Р8	Владеть иностранным языком на уровне, позволяющем работать в иноязычной среде, разрабатывать документацию, презентовать и защищать результаты комплексной инженерной деятельности.
Р9	Эффективно работать индивидуально и в качестве члена группы, состоящей из специалистов различных направлений и квалификаций, демонстрировать ответственность за результаты работы и готовность следовать корпоративной культуре организации.
Р10	Демонстрировать знания правовых, социальных, экономических и культурных аспектов комплексной инженерной деятельности.
Р11	Демонстрировать способность к самостоятельной работе и к самостоятельному обучению в течение всей жизни и непрерывному самосовершенствованию в инженерной профессии.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт: Юргинский технологический институт
Направление подготовки: 20.03.01 «Техносферная безопасность»
Профиль: «Защита в чрезвычайных ситуациях»

УТВЕРЖДАЮ:
Руководитель ООП
_____ С.А. Солодский
«___» _____ 2020 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

БАКАЛАВРСКОЙ РАБОТЫ

Студенту:

Группа	**ФИО**
З-17Г51	Ширяевой Ольге Сергеевне

Тема работы:

Проектирование СКУД на объекте банковской сферы	
Утверждена приказом директора (дата, номер)	от 31.01.2020 г. № 13/С

Срок сдачи студентами выполненной работы:	05.06.2020 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе:	Общие сведения об объекте: филиал ПАО КБ «Восточный», адрес: 652050, Кемеровская обл., г. Юрга, ул. Московская, д. 35. Первый этаж жилого многоквартирного дома. Количество надземных этажей – 5 Класс функциональной пожарной опасности Ф4.3. СОУЭ 1 типа Максимальная вместимость: персонал – до 26 чел.
Перечень подлежащих исследованию, проектированию и разработке вопросов:	1. Изучить зарубежный и отечественный опыт, нормативно-правовую базу в сфере контроля и управления доступом на банковские объекты. 2. Дать характеристику исследуемого объекта и проанализировать состояние безопасности объекта защиты. 3. Разработать проект системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга. 4. Рассчитать экономические затраты на внедрение разработанного проекта.
Перечень графического материала: *(с точным указанием обязательных чертежей)*	1. Схема помещения офиса ПАО КБ «Восточный» (1 лист А3). 2. План расположения оборудования и кабельных трасс (1 лист А3). 3. Схема установки оборудования двери с двусторонним доступом (1 лист А3). 4. Схема установки оборудования двери с односторонним доступом (1 лист А3).

	5. Структурная схема система контроля и управления доступом (1 лист А3).
Консультанты по разделам выпускной квалификационной работы *(с указанием разделов)*	
Раздел	**Консультант**
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Лизунков В.Г., к.пед.н., доцент
Социальная ответственность	Солодский С.А., к.т.н.
Нормоконтроль	Деменкова Л.Г.
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
Реферат	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	10.02.2020 г.

Задание выдал руководитель/ консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ЮТИ ТПУ/ Ст. преподаватель ЮТИ ТПУ	Мальчик А.Г./ Деменкова Л.Г.	к.т.н./ -		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
З-17Г51	Ширяева О.С.		

Реферат

Выпускная квалификационная работа содержит 111 стр., 25 рис., 28 табл., 57 источников, 5 приложений.

Ключевые слова: СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ, БАНКИ, ИДЕНТИФИКАЦИЯ, РАЗГРАНИЧЕНИЕ ДОСТУПА, НАДЕЖНОСТЬ.

Объектом исследования является филиал ПАО КБ «Восточный» в г. Юрга.

Предмет исследования: система контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга.

Цель работы: проектирование системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга.

В процессе исследования проводился анализ систем контроля и управления доступом, применяемых в России и за рубежом, изучение объекта защиты.

В результате выполнения выпускной квалификационной работы разработан проект системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга, соответствующий требованиям нормативных документов.

Выпускная квалификационная работа оформлена в текстовом редакторе Microsoft Word 2007 и представлена в печатном и электронном виде.

Степень внедрения: начальная.

Область применения: безопасность объектов банковской сферы.

Экономическая эффективность и значимость: высокая.

В дальнейшем планируется осуществление более детальной разработки проекта с последующим внедрением.

Abstract

Final qualifying work consists of 11 pages, 25 figures, 28 tables, 56 sources, 5applications.

Keywords: ACCESS CONTROL AND MANAGEMENT SYSTEMS, BANKS, IDENTIFICATION, AUTHENTICATION, AUTHORIZED ACCESS.

The object of the study is a branch of PJSC CB Vostochny in Jurga.

Subject of research: access control and management system of the branch of PJSC CB Vostochny in Jurga.

Purpose of the work: design of the access control and management system of the branch of PJSC CB Vostochny in Yurga.

In the course of the study, the analysis of access control systems used in Russia and abroad, and the study of the object of protection were carried out.

As a result of the final qualification work, a project of the access control and management system of the Vostochny branch of PJSC CB in Yurga was developed that meets the requirements of regulatory documents.

The final qualifying work is designed in the text editor Microsoft Word 2007 and is presented in print and electronic form.

Degree of implementation: initial.

Scope of application: security of objects of the ban sphere.

Economic efficiency and significance: high.

In the future, it is planned to carry out more detailed development of the project with subsequent implementation.

Нормативные ссылки

В настоящей работе использованы ссылки на следующие стандарты:

ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 50862-96 Системы безопасности. Инженерные средства защиты. Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость

ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний

ГОСТ 12.1.004-91 Система стандартов безопасности труда. Пожарная безопасность. Общие требования

ГОСТ 14254-2015 Степени защиты, обеспечиваемые оболочками (коды IP)

ГОСТ 27.002-2015 Надежность в технике (ССНТ). Термины и определения

ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования

ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования

ГОСТ 12.0.003-2015 ССБТ. Опасные и вредные производственные факторы. Классификация

ГОСТ Р 12.1.019-2009 Электробезопасность. Общие требования и номенклатура видов защиты

Оглавление

Введение

Защита любого промышленного предприятия, объекта социальной сферы, коммерческого банка состоит из нескольких рубежей в соответствии с уровнем режимности объекта. Для каждого из перечисленных объектов значимым рубежом считается система контроля и управления доступом (СКУД). Согласно ГОСТ Р. 51241-2008 под СКУД понимают «совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью» [1].

Созданная на основе современных технических средств СКУД позволит решать целый ряд задач, к которым относятся противодействие воровству, саботажу и умышленному повреждению материальных ценностей, учет рабочего времени, контроль трудовой дисциплины и др.

В мире банковского дела всегда существует риск силового вторжения, которое может привести к огромным потерям активов и даже гибели сотрудников. Анализируя данные о преступлениях в банковской сфере, размещённые в пресс-релизах МВД России, за период с 2017 по 2018 гг., отметим, что из 31 наиболее резонансного преступления, совершённого без участия работников банка, 67,7 % (21 случай) представляют собой разбойные нападения с целью завладения наличными; 25,8 % (8 случаев) – кражи наличных из банкоматов [2].

Приведем некоторые данные, основываясь на новостной ленте сайта «Российской газеты» [3]:

- январь 2020 г., г. Чебоксары – попытка ограбления отделения «Совкомбанка»;

- январь 2020 г., г. Вологда – попытка взрыва банкомата при помощи газового баллона, злоумышленник погиб;

- декабрь 2019 г., г.Находка – разбойное нападение на отделение «Сбербанка», ущерб – более 1 млн. руб.;

- апрель 2019 г., г. Кострома – взрыв банкомата при помощи газового баллона, кража 87000 руб., повреждения здания «Сбербанка»;

- июль 2019 г., г. Москва – разбойное нападение на банк «Металлург», ущерб – 136 млн. руб.;

- июль 2018 г., г. Москва – разбойное нападение на банк «Столичный Кредит», ущерб – 12 млн. руб. Поэтому в банковской сфере большое внимание уделяется системам контроля и управления доступом, которые должны иметь надежные решения, которые будут оставаться актуальными и эффективными в течение многих лет.

Следует отметить, что СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом. По данным ряда экспертов [4], ежегодный прирост рынка СКУД составляет более 25 %. В качестве наиболее часто используемых средств контроля и управления доступом в банковской сфере перечислим турникеты, шлюзовые кабины, двери, замки и защёлки, идентификаторы различной природы и др.

Актуальными трендами в современных условиях являются интеграция СКУД с другими системами безопасности, идентификация по смартфону, биометрическая идентификация [5]. В настоящее время пандемия COVID-19 заставляет работодателей задуматься об интеграции систем контроля доступа с тепловизорами, ИК-термометрами с целью автоматизации процесса выявления лиц с повышенной температурой.

Цель выпускной квалификационной работы: проектирование системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга.

Объект исследования: филиал ПАО КБ «Восточный» в г. Юрга.

Новизна работы обуславливается тем, что прежде для исследуемого объекта не проводился анализ существующей системы обеспечения безопасности.

Задачи работы:

- изучить зарубежный и отечественный опыт в сфере систем контроля и управления доступом;

- дать характеристику исследуемого объекта и проанализировать применяемую в настоящее время систему обеспечения безопасности функционирования филиала ПАО КБ «Восточный» в г. Юрга;

- разработать проект системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга для повышения эффективности обеспечения его безопасности;

- рассчитать экономические затраты на внедрение системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга.

Актуальность выбранной темы заключается в том, что совершенствование системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга позволит усилить безопасность работников и клиентов банка, его бесперебойную работу, предупредить потенциальные незаконные вмешательства, сократить материальный ущерб и минимизировать последствия возможной чрезвычайной ситуации.

Область применения результатов работы распространяется также и на другие вводимые в эксплуатацию объекты банковской сферы.

1 Анализ существующих систем контроля и управления доступом

1.1 Общие принципы работы систем контроля и управления доступом

Согласно ГОСТ 51241-2008 системы контроля и управления доступом (СКУД) – это совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью [1].

В соответствии с рекомендациями по выбору и применению систем контроля и управления доступом Р. 78.36.005-2011 [6] в основе работы СКУД заложен принцип сравнения тех или иных идентификационных признаков, принадлежащих или присущих конкретному субъекту (физическому лицу) или объекту (предмету, транспортному средству), с информацией, заложенной в памяти системы.

Понятия идентификатора и идентификации являются основными понятиями для СКУД. Термин идентификация означает – опознавание, поиск по признаку. Идентификация может производиться по следующим основным принципам:

- по коду, вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств;
- по коду, записанному на физическом носителе (идентификаторе) в качестве которого применяются различные ключи, карты, брелоки и т.д.;
- биометрическая идентификация, основанная на определении индивидуальных физических признаков человека.

Каждый из пользователей (сотрудников) получает индивидуальный идентификатор. В качестве такого предмета может быть использована пластиковая карта,брелок, браслет или другой подобный предмет (рис. 1). Идентификатор может быть закреплен также на определенном предмете и транспортном средстве. Пароль, кодовое число, а также предмет-

идентификатор относятся классу присвоенных идентификационных признаков. При этом идентифицируется не сам человек, а присвоенный ему признак.

а б в г

Рисунок 1 – Виды идентификаторов:

а – пластиковая карта; б – браслет; в, г – брелки Touch Memory

В качестве идентификационных признаков могут использоваться присущие признаки человека (биометрические данные) такие как, отпечатки пальцев, геометрия кисти руки, голосовые характеристики и т.д.) (рис. 2).

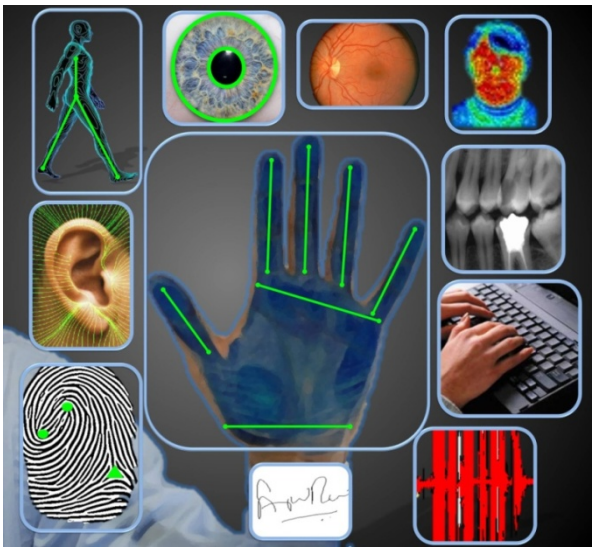


Рисунок 2 – Способы биометрической идентификации

Работа СКУД происходит следующим образом. У входа в контролируемое помещение устанавливаются специальные устройства-считыватели, которые предназначены для считывания информации с идентификатора, ввода пароля или кодового числа, ввода биометрических данных человека. Далее информация поступает на контроллеры доступа, которые на основании анализа данных о владельце обеспечивают управление преграждающими и исполнительными устройствами: открывают или блокируют дверь, включают сигнал тревоги, регистрируют присутствие

человека на рабочем месте и т.д. На рис. 3 представлена общая логическая схема построения системы контроля и управления доступом.

Рисунок 3 – Общая схема работы СКУД

Таким образом, СКУД являются одним из элементов комплексных решений для обеспечения высокого уровня безопасности объекта. Принцип работы СКУД позволяет строго контролировать любые перемещения в зоне действия. В настоящее время СКУД являются одной из ключевых составляющих системы безопасности банка или финансовой организации, оперирующей с крупными суммами наличных или большими объемами драгоценных металлов или камней. Для банка это первая линия защиты, которая позволяет не только предотвратить несанкционированный доступ в помещения банка злоумышленников, но и своевременно идентифицировать факт взлома и подать соответствующий сигнал на пульт службы охраны. В связи с этим подробнее разберём возможности СКУД.

1.2 Обзор возможностей систем контроля и управления доступом

В процессе своей работы, как показано в Р 78.36.005-2011 [6] СКУД должна выполнять следующие функции:

- санкционирование – процедура присвоения каждому пользователю персонального идентификатора, кода, регистрацию его в системе (или регистрацию его биометрических признаков);

- задание для пользователя временных интервалов и уровня доступа (в какие помещения, когда и кто имеет право заходить);

- идентификация – процедура опознавания пользователя по предъявленному идентификатору или биометрическому признаку;

- авторизация – проверка полномочий, заключающаяся в проверке соответствия времени и уровня доступа установленным в процессе санкционирования;

- аутентификация – установление подлинности пользователя по признакам идентификации;

- разрешение доступа или отказ в доступе – выполняется на основании результатов анализа предыдущих процедур;

- регистрация – протоколирование всех действий в системе;

- реагирование – реакция системы на несанкционированные действия (подача предупреждающих и тревожных сигналов, отказ в доступе и т.д.).

Процедура санкционирования производится оператором или администратором системы, все остальные процедуры могут производиться системой автоматически. Очевидно, что процедура аутентификации может быть выполнена полноценно только с помощью биометрических систем [7].

Итак, системы контроля и выполнения доступом не только предотвращают проникновение любых нежелательных людей на охраняемую территорию, но и обеспечивают целостность и защиту материальных ценностей, важной информации, гарантируют безопасность для персонала и посетителей. Отметим важность для выявления нарушений трудовой дисциплины таких функций, как отслеживание перемещения всех сотрудников в офисе, учёт и фиксация отработанного сотрудниками времени (данные о прогулах, опоздавших, ушедших с работы раньше времени и т.п.).

Основными наиболее востребованными на практике функциями СКУД, особенно на объектах банковской сферы являются [8]:

- разграничение доступа к закрытым внутренним помещениям;

- учет рабочего времени и контроль своевременного прихода персонала на работу в интеграции с платформами бухгалтерского учёта («1С: Бухгалтерия», «Парус», БЭСТ-3 и др.).

Более совершенные и дорогостоящие системы контроля и управления доступом имеют дополнительные функциональные возможности [9]:

- возможность получения единовременного доступа по отпечатку пальцев в конкретное помещение здания;

- управление исполнительными устройствами в автоматическом режиме в соответствии с ранее составленными расписаниями;

- возможность работы с разовыми или временными электронными пропусками;

- возможность совместной работы с настольными считывателями для более полного контроля использования служащими рабочего времени;

- отображение интерактивных планов объекта, его текущего состояния и возможностью общего управления однотипными устройствами (открытие или блокировка по тревоге) и др.

Представленная на рис. 4 схема СКУД PERCo-S-20 [10] многофункциональна.

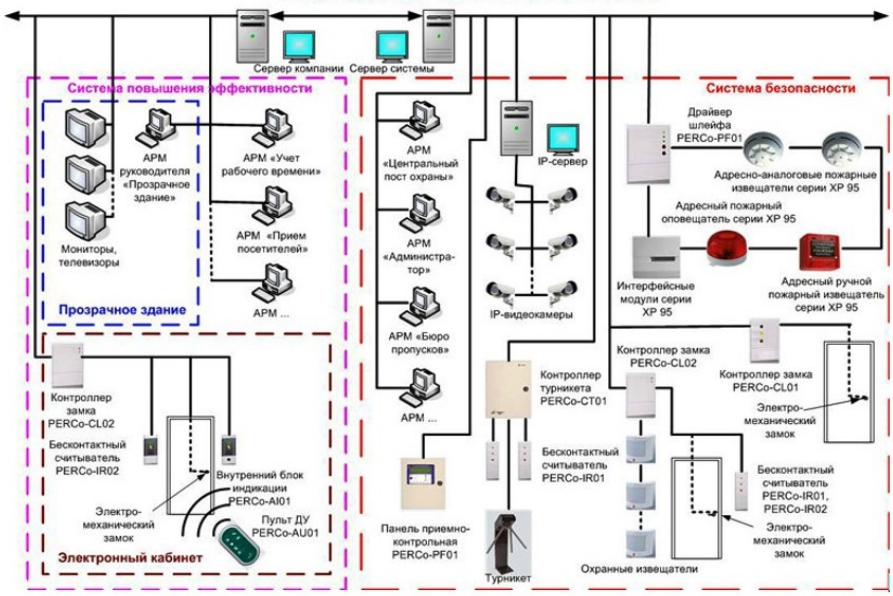


Рисунок 4– Структурная схема СКУД PERCo-S-20

В сети СКУД связь осуществляется по интерфейсу Ethernet. В качестве идентификаторов используются бесконтактные (Proximity) карты и брелоки. В качестве исполнительных устройств в СКУД PERCo-S-20 могут использоваться турникеты, калитки, электромагнитные и электромеханические замки. Наличие

в контроллерах доступа встроенной поддержки шлейфов охранной сигнализации позволяет контролировать весь объем помещения. Как видно на рис. 4, система обеспечения безопасности интегрирована с системой повышения эффективности трудовой деятельности.

На данный момент существует огромное количество разных типов систем контроля и управления доступом, которые отличаются степенями надежности, сложностью настройки и обслуживания, стоимостью, но, как правило, выполняют следующие основные функции: обнаружение, опознавание, управление, контроль, которые представлены в виде схемы на рис. 5.

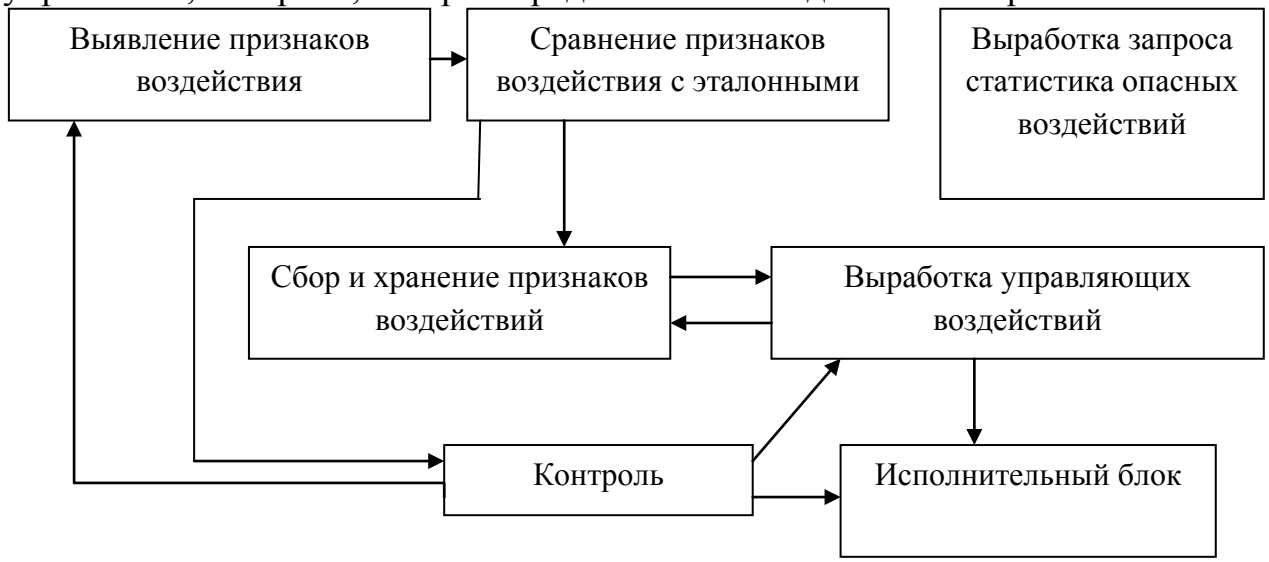


Рисунок 5 – Функциональная схема системы контроля и управления доступом

Архитектура СКУД, представляющая собой гибкую, модульную систему, позволяет выбрать из имеющихся на рынке именно тот комплект оборудования, который будет оптимально отвечать потребностям предприятия и может быть впоследствии модернизирован. В свете этого рассмотрим компонентный состав систем контроля и управления доступом.

1.3 Основные компоненты системы контроля и управления доступом

Основными компонентами систем контроля и управления доступом являются средства контроля и управления доступом (средства КУД) – механические, электромеханические, электрические, электронные устройства,

конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом (рис. 6) [1].

В соответствии с Р. 78.36.005-2011 [6] средства контроля и управления доступом классифицируются по функциональному назначению устройств; функциональным характеристикам; устойчивости к несанкционированному доступу (НСД).

Рисунок 6 –Примеры средств контроля и управления доступом

Средства КУД по функциональному назначению устройств подразделяются на преграждающие управляемые (УПУ), исполнительные, считывающие устройства, идентификаторы и средства управления в составе аппаратных устройств и программных средств.

УПУ – устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, проходные кабины, двери и ворота, оборудованные исполнительными устройствами систем контроля и управления доступом) [6] (рис. 7). В состав СКУД могут входить дополнительные средства, предназначенные для обеспечения работы СКУД (блоки бесперебойного питания; датчики состояния УПУ; дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления УПУ; устройства преобразования интерфейсов сетей связи; аппаратура передачи данных по различным каналам связи и др.).

Компонентами СКУД являются также аппаратно-программные средства – средства вычислительной техники (СВТ) общего назначения (компьютерное

оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

Рисунок 7– Примеры УПУ

По функциональным характеристикам УПУ классифицируются по виду перекрытия проема прохода:

- с частичным перекрытием (турникеты, шлагбаумы);

- с полным перекрытием (полноростовые турникеты, специализированныеворота);

- со сплошным перекрытием проема (сплошные двери, ворота);

- с блокированием объекта в проеме (шлюзы, кабины проходные).

Исполнительные устройства классифицируются по способу запирания на электромеханические и электромагнитные замки; электромагнитные защелки; механизмы привода дверей, ворот.

Устройства ввода идентификационных признаков (УВИП) – электронные устройства, предназначенные для ввода и считывания кодовой информации с идентификаторов. В состав УВИП входят считыватели и идентификаторы. Считыватель – устройство в составе УВИП, предназначенное для считывания идентификационных признаков и передачи этой информации в контроллер системы контроля и управления доступом (рис. 8).

Рисунок 8 – Считыватель ST-11

Идентификатор пользователя – уникальный признак субъекта или

объекта доступа. В качестве идентификаторов используются магнитные карточки, бесконтактные proximity-карты, брелки, различные радиобрелки, а также различные физические признаки конкретного человека, как например изображение радужной оболочки глаза, отпечаток пальца или отпечаток ладони.. В настоящее время применяются следующие типы карт:

- бесконтактные радиочастотные (proximity) карты – наиболее перспективный тип карт. Бесконтактные карточки срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу и удобство использования, высокую пропускную способность. Считыватель генерирует электромагнитное излучение определенной частоты и, привнесении карты в зону действия считывателя, это излучение через встроенную в карте антенну запитывает чип карты. Получив необходимую энергию для работы, карта пересылает на считыватель свой идентификационный номер с помощью электромагнитного импульса определенной формы и частоты;

- магнитные карты – наиболее широко распространенный вариант. Карты Виганда (Wiegand) названы по имени ученого, открывшего специальный сплав, обладающий магнитными свойствами, которые трудно дублировать. Внутри карты расположены отрезки проволоки из этого сплава. Карта может быть контактной и бесконтактной и считывается путем поднесения или пропускания через терминал, называемый считыватель Wiegand. Эти карты более долговечны, достаточно безопасные и обеспечивают максимальную защиту от подделки, но и более дорогие. Один из недостатков – то, что код в карту занесен при изготовлении раз и навсегда;

- штрих-кодовые карты – на карту наносится штриховой код;

- ключ-брелок – металлическая таблетка, внутри которой расположен чип постоянного запоминающего устройства. При касании таблеткой считывателя из памяти таблетки в контроллер пересылается уникальный код идентификатора.

Идентификаторы и считыватели классифицируются по следующим признакам:

- по виду используемых идентификационных признаков (идентификаторы и считыватели);

- по способу считывания идентификационных признаков (считыватели).

По виду используемых идентификационных признаков идентификаторы и считыватели могут быть:

- механические – идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

- магнитные – идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);

- оптические – идентификационные признаки представляют собой нанесенные на идентификатор метки, имеющие различные оптические характеристики (карты со штриховым кодом, голографические метки ит.д.);

- электронные контактные – идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);

- электронные радиочастотные – электронные идентификаторы, считывание кода с которых происходит путем передачи данных по радиоканалу;

- акустические – идентификационные признаки представляют собой кодированный акустический сигнал;

- биометрические (только для считывателей) – идентификационные признаки представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);

- комбинированные – для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыватели могут быть с ручным вводом, контактные, бесконтактные, комбинированные.

Средства управления – устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с устройств идентификации, управление преграждающими устройствами, отображение и регистрацию информации. Классификация средств управления СКУД включает в себя: аппаратные средства (устройства) – контроллеры доступа (приборы приемно-контрольные доступа); программные средства – программное обеспечение СКУД.

Все устройства в системе общаются между собой по определённым правилам, которые называются протоколами. Существуют стандартные протоколы, и это позволяет использовать в одной системе оборудование разных производителей. Программное обеспечение осуществляет настройку и управление оборудованием, мониторинг его параметров, систематизацию и архивирование всей информации системы.

Контроллеры – основа аппаратной части системы, к ним подключается необходимое дополнительное оборудование: считыватели, интерфейсные модули, замки, герконы (дверные контакты), кнопки выхода, охранные датчики и прочее периферийное оборудование. По способу управления контроллеры системы контроля и управления доступом делятся на три класса:

- сетевые контроллеры подразумевают возможность работы контроллеров в сети под управлением компьютера (рис. 9),;

Рисунок 9 – Сетевые контроллеры

- автономные контроллеры – устройства, предназначенные для обслуживания, как правило, одной точки прохода (рис.10).

Рисунок 10 – Автономный контроллер СКУД Z-5R 5000

Встречаются самые разнообразные вариации: контроллеры, совмещенные со считывателем, контроллеры, встроенные в электромагнитный замок и так далее. Автономные контроллеры рассчитаны на применение самых разных типов считывателей. Как правило, автономные контроллеры рассчитаны на обслуживание небольшого количества пользователей, обычно до пятисот;

- комбинированные контроллеры объединяют функции сетевых и автономных контроллеров (рис. 11). При наличии связи с управляющим компьютером контроллеры работают как сетевое устройство, при отсутствии связи – как автономные.

Рисунок 11 –Комбинированные контроллеры

Считав информацию с карты (или другого устройства идентификации), контроллер сверяет её со своей базой данных и принимает решение: давать или не давать команду на исполнительное устройство – замки, турникеты, шлагбаумы, калитки.

На рис. 12 показана схема устройства системы контроля и управления доступом. Системы КУД классифицируют по способу управления, количеству контролируемых точек доступа, функциональным характеристикам, уровню защищенности системы от несанкционированного доступа к информации. По количеству контролируемых точек доступа системы КУД бывают: малой

емкости (до 64 точек);средней емкости (от 64 до 256 точек);большой емкости (более 256 точек).

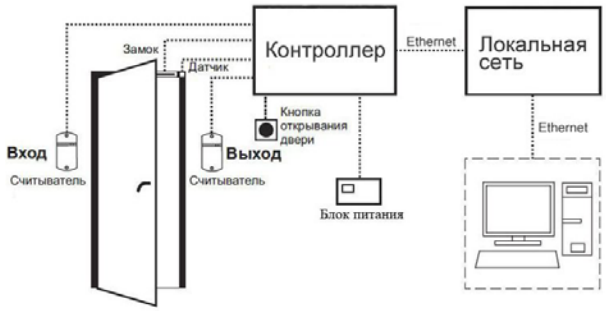


Рисунок 12 – Схема устройства системы контроля и управления доступом

По способу управления системы КУД могут быть:

- автономные – для управления одним или несколькими УПУ, без передачи информации на центральное устройство управления и без контроля со стороны оператора;

- сетевые – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;

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

По функциональным характеристикам системы КУД могут быть трех классов: с ограниченными и расширенными функциями, а также многофункциональные.

Классификация средств КУД по устойчивости к несанкционированному доступу (НСД) определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости: нормальной; повышенной; высокой. УПУ классифицируют по устойчивости к разрушающим воздействиям: взлому, пулестойкости (только для УПУ со сплошным перекрытием проема), устойчивости к взрыву. Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции. Для УПУ повышенной

и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и с блокированием объекта в проёме(шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости.

Устройства исполнительные (замки, защелки) классифицируют по устойчивости к разрушающим воздействиям в зависимости от конструкции.

По устойчивости к неразрушающим воздействиям средства КУД в зависимости от их функционального назначения классифицируют по устойчивости к вскрытию, манипулированию, наблюдению для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п.), копированию (для идентификаторов), защите средств вычислительной техники (СВТ) средств управления СКУД от несанкционированного доступа к информации.

Ознакомление с компонентным составом СКУД позволяет перейти к их рассмотрению опыта их проектирования.

1.4 Российский и зарубежный опыт проектирования систем контроля и управления доступом

Возросшее стремление предприятий и организаций к обеспечению безопасности в XXI веке послужило мощным катализатором разработки новых технических средств и программного обеспечения для систем контроля и управления доступом. Такая тенденция положительно повлияла на рынок СКУД, так как выросло число предложений и покупателей, снизилась их цена [11]. Вместе с тем многообразие предложений существенно усложняет выбор конкретной модели и производителя [12].

Российский рынок систем контроля доступа характеризуется достаточно высокой конкуренцией между производителями, насчитывая несколько сотен отечественных и иностранных производителей. Приведём данные анализа их популярности по оценке Яндекс. Данные поиска за февраль 2020 г.

представлены в табл. 1. Анализ представленных результатов позволяет прийти к следующему выводу: если контроллеры практически для всех производителей имеют одинаковую стоимость, то программное обеспечение может быть как бесплатным, так и представлять довольно значительную статью расходов. Статистика показов также подтверждает [18],что потребители стали покупать более дорогие системы обеспечения безопасности.

Таблица 1 – Сравнительный анализ российских производителей СКУД

Производитель	Популярность, показов/месяц	Стоимость, руб.	
		Контроллер	Программное обеспечение
Hikvision	56963	от 7 659	от 52 000
PERCo	27713	от 6 227	от 0 до 96 000
Bolid	18527	от 5 483	от 39 000
Parsec	13720	от 6 960	от 41 000
Octagram	12586	от 7 024	от 41 574
RusGuard	6576	от 1 890	от 0 до 29 000
Эра новых технологий	960	от 3 660	от 0 до 19 000

Рассмотрим данные анализа сферы СКУД, полученные при опросе экспертов [13]. Популярные технологические тренды (рис. 13) участники опроса распределили в таком порядке (от самого важного к менее значимому):

- биометрическая идентификация;
- рост роли интеграционных платформ;
- рост популярности IP-технологий;
- развитие технологий мобильного доступа;
- переход на защищенные протоколы передачи данных в идентификаторах;
- автоматизация;
- учет рабочего времени.

Этими же экспертами был определён топ-10 российских компаний – производителей СКУД: Болид (СКУД ИСО «Орион»); PERCo (СКУД PERCo); SIGUR (СКУД SIGUR); Релвест (СКУД Parsec);AAM Системз (APACS 3000, Lyrix); Рубеж (СКУД «Рубеж»); IronLogic (СКУД IronLogic); Smartec (СКУД Smartec); Прософт Биометрикс (СКУД Biosmart); Равелин (СКУД Gate).

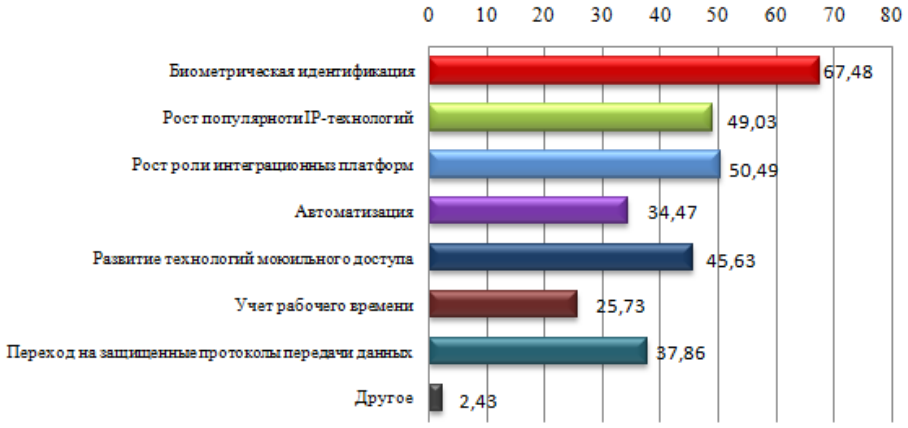


Рисунок 13 – Ключевые технологические тренды СКУД

Среди зарубежных компаний, присутствующих на российском рынке, лидирующими были названы: HID Global; Honeywell Security (Northern Computers); APOLLO; Bosch Security Systems; Siemens; Axis Communications. При оценке результатов опроса об известности брендов следует, конечно, помнить о разных рыночных сегментах, в которых они работают.

Приведём пример популярных решений СКУД ряда зарубежных производителей [5]. Все они основаны на перспективном направлении развития СКУД – доступе по смартфону. Современные системы доступа по смартфону – это решения, сочетающие удобство использования мобильных идентификаторов с простотой и надёжностью традиционных «карточных» СКУД. Достоинства этого способа очевидны: смартфон всегда с собой, его не передают приятелям или коллегам, он имеет собственные средства защиты (пароль, графический рисунок, биометрическая защита). Важной составляющей работы СКУД с идентификацией по смартфону является мобильное приложение, которое можно бесплатно установить в Play Market или Appstore. В табл. 2 приведено сравнение приложений для мобильного доступа ведущих российских производителей СКУД [14].

Таблица 2 –Сравнение приложений для мобильного доступа ведущих российских производителей СКУД

Название	Платформы	Передача данных	Создание идентификаторов	Отзыв идентификатора	Способ передачи идентификатора контроллеру
ESMART. Доступ	Apple, Android	BLE, NFC	Платный виртуальный идентификатор	По истечении заданного срока деактивируется	По e-mail в виде файла формата .xlsx с паролем
Parsec Card Emulator	Android	NFC	Генерируется на основе IMEI	Выдается как постоянный, затем деактивируется вручную	Администратор получает идентификатор от владельца смартфона и вводит его в систему
PERCo. Доступ	Android, для работы с устройствами Apple приложение не нужно	NFC	IMSI – для Android, Token – для в Apple		
Proxway Mobile ID	Apple, Android	BLE, NFC	Бесплатный генерируется на основе данных смартфона, платный – на сервере производителя	Выдается в обычном режиме, затем деактивируется вручную	Администратор системы получает код активации по e-mail в виде файла формата .xlsx с паролем
RusGuard Key	Android	NFC	Генерируется на основе IMEI смартфона		Администратор получает идентификатор от владельца смартфона и вводит его в систему
Sigur. Доступ	Apple, Android	BLE, NFC	Генерация на стороне устройства, обеспечивающего уникальность ID		Виртуальный идентификатор передается в систему от смартфона

Мобильные приложения являются одним из развивающихся трендов рынка, т.к. позволяют использовать смартфон как идентификатор и регистрирующее устройство. Системы с таким способом идентификации предназначены для работы в условиях, где поставить контроллер регистрации не представляется возможным, а контроль доступа и учет сотрудников крайне важен: например, на объектах с повышенными требованиями к безопасности, в т.ч. и на крупных объектах банковской сферы. По мнению экспертов [13], рынок мобильной идентификации в будущем продолжит активно расти: к

концу 2020 г. прогнозируется доля идентификации по смартфону для СКУД составит 20%.

1.5 Особенности систем контроля и управления доступом в банковской сфере

В банках, работающих с физическими лицами, требования к безопасности заведомо более серьезны, чем в большинстве организаций. На таких объектах всегда существует риск силового вторжения, которое может привести к огромным потерям активов и даже гибели сотрудников. К специфично банковским требованиям относится, например, введение временных задержек при доступе в критически важные зоны. Должна быть функция регистрации действий по силовому демонтажу банкомата. Для этого обычно используются реагирующие на вибрацию сейсмические датчики. Каждый сейсмический извещатель способен обезопасить до 80 $м^2$ стены [15]. Это весьма экономный и эффективный способ защиты.

Кроме того, в традиционных офисных сигнализациях обычно есть одна клавиатура или аналогичное устройство, позволяющее включать и выключать режим охраны. В банках ставить систему на охрану можно также с одной клавиатуры, но снятие с охраны производится последовательно для разных помещений. Могут быть разные логические схемы снятия помещений с охраны [16].

Злоумышленники (например, при вооруженном налете) могут проникнуть в банк под видом простых клиентов, и система должна обладать возможностями для противодействия такому нападению. Обычно для этого ставят ручные охранные извещатели («тревожные кнопки»). Подать сигнал тревоги с их помощью можно рукой или ногой. Такие извещатели передают на пульт мониторинга тревожный сигнал вне зависимости от того, поставлена ли система на охрану. Часто применяются беспроводные ручные и автоматические охранные извещатели [17].

На объектах банковской сферы следует минимизировать количество ложных срабатываний. Одним из общепринятых решений является следующее: установленные в помещениях пассивные инфракрасные извещатели не генерируют «полного» тревожного сигнала, который передается на пульт охраны. Информация о срабатывании сохраняется локально. Если менеджер, придя на работу, видит желтый или красный свет, ему следует вызвать поддержку перед тем, кто войти охраняемую зону.

Другой способ борьбы с ложными срабатываниями – использование фильтрующего центра, который обслуживается банком самостоятельно. У сотрудников центра есть по 90 с на оценку и отмену каждого тревожного сигнала [18]. Если же интервал истек, то извещение охранной системы транслируется в полицию. Установлено, что применяемые в настоящее время в банках методы снижения доли ложных тревог оказались очень эффективными. Сейчас из тех тревожных уведомлений, которые доходят до полиции, ложными оказываются менее 1% [18].

Согласно Р 78.36.003-99 « Рекомендации по комплексному оборудованию банков … техническими средствами охраны, видеоконтроля и инженерной защиты. Типовые варианты» [19] техническая укрепленность объекта банковской сферы должна быть достаточной для обеспечения защиты помещений от проникновения преступников на время, необходимое для выявления и пресечения нарушения; хранимых денежных и материальных ценностей от хищений с использованием квалифицированных методов взлома; персонала объекта и посетителей от вооруженных нападений.

Подготовка и выполнение работ по усилению технической укрепленности банков должны осуществляться в соответствии с нормативными документами МВД России:

- РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ» [20];

- РД 78.147-93 «Единые требования по технической укрепленности и оборудованию сигнализацией объектов» [21].

В зависимости от вида и концентрации ценностей, размещенных на объекте, объекты и помещения подразделяются на четыре категории, а строительные конструкции (стены, оконные проемы, двери) данных объектов (помещений) – на четыре группы (классы) защиты от взлома.

Анализируемый объект относится к помещениям, в которых размещаются материальные ценности второй категории – помещения с постоянным и временным хранением денежных средств, валюты и ценных бумаг, секретной документации и т.п., утрата которых может принести значительный материальный и финансовый ущерб, создать угрозу здоровью и жизни людей, находящихся на объекте.

Наружные стены таких объектов и помещений, должны иметь группу защиты от взлома не ниже третьей: высокая степень защиты от взлома, используются каменные, кирпичные, блочные, бетонные и пустотные железобетонные конструкции толщиной более 500 мм.

Все помещения внутри объекта разделяются на три основные зоны по доступности:

- первая зона – помещения, доступ в которые для сотрудников и клиентов не ограничен (операционный зал банка);

- вторая зона – помещения, доступ в которые разрешен ограниченному кругу сотрудников (служебные);

- третья зона – помещения, доступ в которые имеют лишь строго определенные должностные лица объекта (например, кладовые и сейфовые комнаты банков, кассовые кабины, помещения подразделений охраны).

Помещения второй зоны доступности следует отделять от помещений первой зоны стенами и перегородками второй группы защиты от взлома. Помещения третьей зоны доступности от помещений второй зоны также следует отделять стенами и перегородками второй группы защиты от взлома. Между помещениями первой и третьей зон доступности должны предусматриваться стены или перегородки третьей группы защиты от взлома.

Входные двери на объекты (в помещения), должны иметь группу защиты от взлома не ниже третьей (высокая степень защиты от взлома) [26], обычно это металлические стальные двери с толщиной листа не менее 4 мм.

Защитное остекление должно быть класса Б1 (устойчивость к пробиванию отверстия, достаточного для проникновения человека ударами топора, минимальное количество ударов топором: 30–50) согласно РД 78.148-94 [22], а оконные проемы первого этажа объекта должны иметь группу защиты от взлома не ниже третьей (высокая): окна специальной конструкции с защитным остеклением класса А3 и выше.

Механизмы замков должны быть заключены в кожухи, защищающие их и подходящие провода от умышленных повреждений с использованием ручного слесарного инструмента. Входную дверь на объект рекомендуется оборудовать электромеханическими и/или механическими замками с количеством комбинаций кода (ключа) не менее 100000.

Вход из операционного зала в служебные помещения, в кассы должен быть оборудован дверями, имеющими конструкцию, группа защиты от взлома которых не ниже второй. Замки дверей должны иметь защиту от подбора ключей и использования отмычек.

Хранение особо важных материальных ценностей рекомендуется производить в специально приспособленных для этих целей кладовых или в сейфах. В соответствии с ГОСТ Р. 50862-96 «Системы безопасности. Инженерные средства защиты. Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость» [23] сейф – устройство, предназначенное для хранения ценностей документов и носителей информации с площадью основания изнутри не более 2 м и устойчивое к взлому.

Операционно-кассовый зал, как правило, состоит из разделяемых барьером зоны для клиентов и операционной зоны. Операционные кассы (кассовые кабины) отделяются от зоны клиентов кассового зала барьером, имеющим на высоте 1150 мм горизонтальную панель шириной не менее 400 мм

для работы клиентов с документами. Допускается установка пулезащитного барьера по всему фронту операционной зоны. Устройство проходов из зоны клиентов в закассовое пространство не допускается. Кассовые кабины должны оборудоваться специальными транспортирующими устройствам; (бункерами) или лотками для передачи денег и документов.

Состав, размещение и площади помещений охраны и внутренней службы безопасности объекта согласовываются с местными органами вневедомственной охраны МВД РФ. Объект следует оборудовать системой контроля доступа, предназначенной для: ограничения доступа сотрудников и посетителей объекта в охраняемые помещения; фиксации времени прихода и ухода каждого сотрудника; получения информации об открытии внутренних помещений (когда и кем открыты); выдачи информации о попытках несанкционированного проникновения в помещения объекта и др.

Структурно система контроля доступа должна состоять из следующих компонентов: карточки-пропуска (магнитные, виганд - и проксимити-карты); считыватели; электромагнитные замки и защелки; персонального компьютера с программным обеспечением.

Системой контроля доступа рекомендуется оборудовать все входы на объект и внутренние двери по усмотрению руководства и службы безопасности объекта. Размещение и монтаж технических средств, выбор проводов и кабелей следует производить в соответствии с Р. 78.36.003-99 [19], технической документацией на применяемое изделие, ПУЭ [24].

Шлейфы охранной и тревожной сигнализации, магистральные линии питания постоянного тока следует проводить скрытым способом в стальных трубах и металлорукавах, проложенных в полу или стенах, открытым способом за подвесным потолком. При необходимости прокладки этих проводов и кабелей на расстоянии менее 0,5 м от силовых и осветительных проводов они должны иметь защиту от наводок. Прокладка проводов шлейфа сигнализации, присоединяемых к извещателям, выполняется как скрыто, так и открыто в соответствий с проектом или актом обследования.

Источники резервного электропитания питания следует устанавливать в помещении охраны или другом специально выделенном помещении, при условии, что оно находится под охраной. Для обеспечения работоспособности аппаратуры в аварийных ситуациях должна обеспечиваться работа технических средств в течение не менее 4 ч в дежурном режиме и в течение не менее 1 ч в режиме тревоги.

Перечисленные меры безопасности свидетельствуют о значимости систем контроля и управления доступом для объектов банковской сферы.

1.6 Выводы по главе 1

В данной главе были рассмотрены общие принципы работы СКУД и проанализированы их основные возможности. Приведены главные компоненты систем контроля и управления доступом, выявлена востребованность СКУД на объектах банковской сферы. Анализ российского и зарубежного опыта проектирования систем контроля и управления доступом позволил определить современные тенденции в сфере СКУД: интерес к новым технологиям (мобильный доступ, биометрия), интеграция систем безопасности.

Обзор особенностей систем контроля и управления доступом в банковской сфере, нормативной базы по их проектированию выявил необходимость установки СКУД в офисах банков. Следовательно, необходимо спроектировать систему контроля и управления доступом согласно всем нормативным документам, регламентирующим безопасность банковских объектов, анализ которых также был предпринят в данной главе.

Изучив актуальные тенденции в области СКУД как в России, так и за рубежом, считаем необходимым использовать в проекте оборудование, приборы и материалы, отвечающие современным требованиям, в т.ч. таким аспектам, как эффективность, оптимальная стоимость, ремонтопригодность и возможности модернизации.

2 Общая характеристика объекта исследования

2.1 Характеристика ПАО КБ «Восточный» и его деятельности

Объектом исследования является филиал ПАО КБ «Восточный» в г. Юрга. Предмет исследования: система контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга. При написании выпускной квалификационной работы проводилось изучение нормативно-правовой базы, регламентирующей организацию безопасности объектов банковской сферы; анализ опыта организации систем безопасности банков и, в частности, на объекте защиты.

Филиал ПАО КБ «Восточный» является одной из важнейших финансовых организаций в г. Юрга. Основу деятельности филиала составляет кредитование населения, а главными розничными продуктами являются: первичные нецелевые кредиты, автокредитование, кредиты на ремонт, кредитные карты.

Офис банка расположен по адресу: 652050, Кемеровская область, город Юрга, улица Московская, дом 35 (рисунок 14).

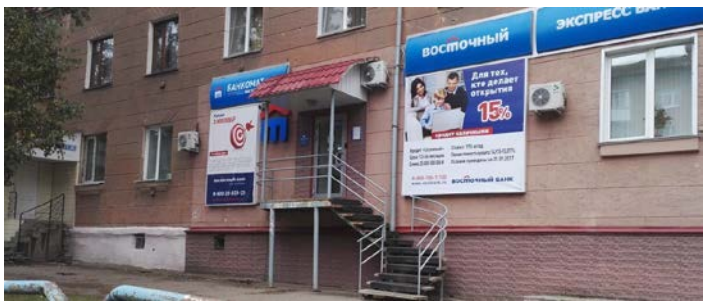


Рисунок 14 – Общий вид здания офиса банка

Отделение банка рассматриваемого объекта располагается в пятиэтажном жилом доме на первом этаже. Площадь объекта составляет 269 м^2. Филиал имеет отдельный вход, независимый от собственников жилья. Общее число работников, включая вспомогательный персонал, составляет 26 чел., одновременно в помещении находится 8 чел.

Филиал ПАО КБ «Восточный» в г. Юрга включает в себя следующие основные помещения: вестибюль с постом охраны, зал для посетителей, кабинет управляющего, касса, кабинеты кредитных экспертов и бытовое помещение с санузлом. План объекта представлен на рисунке 15.

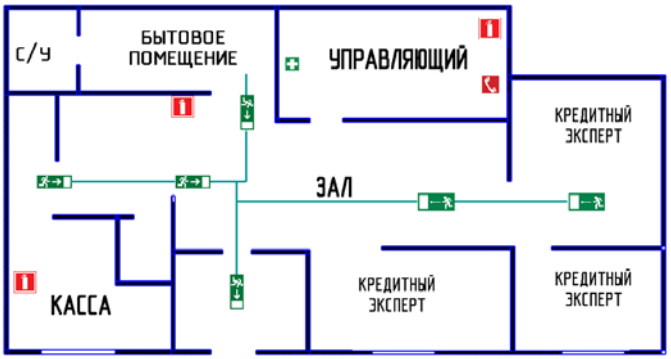


Рисунок 15 – План объекта

В настоящее время средняя посещаемость офиса банка составляет около 40 человек в день, или 5 человек в час.

Согласно Постановлению Правительства РФ от 25.04.2012 № 390, п. 5 [25] филиал ПАО КБ «Восточный» в г. Юрга не относится к объектам с массовым пребыванием людей, т.е. тем, на которых может одновременно находиться 50 и более человек. На объекте в наличии планы эвакуации людей при пожаре с обозначенными местами хранения первичных средств пожаротушения (рис. 15).

Физическая охрана осуществляется сотрудниками охраны филиала ПАО КБ «Восточный» в г. Юрга в рабочее время. Пост охраны расположен в фойе банка. Физическая охрана предназначена для обеспечения безопасности клиентов и персонала банка, соблюдения общественного порядка на объекте, сохранности имущества банка, финансов и ценностей.

Учитывая пределы огнестойкости строительных конструкций здания (несущих и ненесущих стен, перекрытий и др.) согласно СНиП 21-07-97 «Пожарная безопасность зданий и сооружений» [26] здание, в котором находится офис банка, имеет II степень огнестойкости (кирпичные дома), класс функциональной пожарной опасности учреждений банка, контор, офисов – Ф 4.3, класс конструктивной пожарной опасности С0.

Пожарная нагрузка в помещениях филиала ПАО КБ «Восточный» в г. Юрга представляет собой мебель, инвентарь, оборудование и другие материалы. В здании применяются основные строительные конструкции (табл. 3) с пределами огнестойкости и классами пожарной опасности, и строительные материалы с показателями пожарной опасности, соответствующие требованиям.

Таблица 3 – Строительные конструкции и пределы их огнестойкости

Конструкция	Материал	Предел огнестойкости, ч
Наружные и внутренние стены	Кирпич	5,5
Лестницы, перекрытия	Железобетон, плиты	3–5,5

Помещение офиса банка имеет объемно-планировочное решение и конструктивное исполнение путей эвакуации, обеспечивающих безопасную эвакуацию людей при пожаре. Имеется один эвакуационный выход, ведущий из помещений наружу. Эвакуационные пути и проходы содержатся в надлежащем состоянии.

Напряжение электросетей 380/220 В, их эксплуатация, а также контроль за техническим состоянием осуществляется в соответствии с требованиями нормативных документов по электроэнергетике специализированной организацией, имеющей на данный вид деятельности соответствующую лицензию.

2.2 Анализ системы безопасности в филиале ПАО КБ «Восточный»

Для обеспечения безопасности функционирования исследуемого объекта используются, кроме физической охраны, системы контроля и управления доступом, охранного видеонаблюдения, охранной сигнализации, пожарной сигнализации.

Вход и выход работников банка происходит через основной выход, оборудованный охранной сигнализацией. В установленное время перед началом рабочего дня сотрудник охраны в присутствии управляющего

(заместителя управляющего) филиалом банка осуществляет снятие помещения с охранной сигнализации, открывая его. Факт вскрытия фиксируется в журнале за двумя подписями. Далее сотрудник охраны контролирует прохождение работников банка на рабочие места, оставаясь на месте в течение рабочего дня. Автоматическое идентифицирование личности работников не производится, записи в системе учёта рабочего времени не осуществляются. Если в течение рабочего дня сотруднику необходимо неоднократно входить и выходить, то затруднительно оценить время пребывания его в отделении банка. Следовательно, очевидна необходимость оптимизации системы контроля и управления доступом для повышения контроля пропускного и внутриобъектового режима.

При оснащении банка системой видеонаблюдения применялся принцип тотального контроля всей территории. В систему охранного видеонаблюдения в отделении банка входят:

- восемь IP-камер (семь внутренних «Beward B1210R F12», производитель – НПП «Beward», г. Красноярск; одна уличная Falcon Eye FE-IB720MHD/20M-2,8, производитель – компания «Falcon Eye», Китай);
- источник бесперебойного питания Back-UPS BK650EI (650 ВА) (производитель – «APC by Schneider Electric», США);
- коммутатор TL-SG105E(производитель компания «TP-LINK», Китай);
- сервер с программным обеспечением, где записывается и архивируется информация с камер видеонаблюдения.

Несанкционированное проникновение на объект система охранной сигнализации банка детектирует с помощью магнитоконтактных извещателей в количестве 4 шт. Для блокировки дверных проемов на открывание или смещение используются точечные магнитоконтактные охранные извещатели ИО 102-14, производитель ООО НПКФ «Комплектстройсервис», г. Рязань (рис. 16).

Рисунок 16 – Точечные магнитоконтактные охранные извещатели ИО 102-14

Извещатель конструктивно состоит из двух блоков: исполнительного (магнитоуправляемого датчика) и задающего (управляющего магнита), заключенных в пластмассовые корпуса по форме близкой к прямоугольной. С магнитоуправляемого датчика выведены два многожильных провода для подключения извещателя к шлейфу сигнализации, полярность подключения извещателей значения не имеет.

Для блокировки оконных проёмов используются извещатели охранные поверхностные звуковые типа ИО329-10 «Стекло-4» (производитель ЗАО «Риэлта», г. Санкт – Петербург) в количестве 4 шт.(рис. 17).

Рисунок 17 – Извещатели охранные поверхностные звуковые ИО329-10 «Стекло-4»

Исследуемый объект оснащён системой пожарной сигнализации в соответствии с НПБ 110-03 «Перечень зданий и сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией» [27], РД 78-145-93 [20], и НПБ 104-03[28]. Учитывая пожарную нагрузку, на исследуемом объекте смонтированы адресные дымовые оптико-электронные извещатели ИП 212-60А (Леонардо-О) (рис. 18) в количестве 8 шт.Производитель – ООО «Систем Сенсор Технолоджи», г. Москва. Для приема сообщений по адресной шине от извещателей используется адресный модуль АМ-99, который обеспечивает питание и контроль режима работы извещателя по двухпроводной адресной

шине и формирует сигнал для приемно-контрольного прибора «Сигнал–20П» (производитель НВП «Болид», Московская обл.).

Рисунок 18 – Дымовой оптико-электронный извещатель ИП 212-60А (Леонардо-О)

Для оповещения персонала о пожаре во всех помещениях (с постоянным или временным присутствием людей) установлены светозвуковые оповещатели «Свирель-2» (рис. 19). Изготовитель: АО «Радий», Челябинская обл.

Рисунок 19 – Светозвуковой оповещатель «Свирель-2»

Уровень сигнала на расстоянии 1 м от оповещателя – 105 дБ. Оповещатели подключают к приёмно-контрольному прибору «Сигнал-10», (производитель НВП «Болид», Московская обл.).

Для обеспечения системой бесперебойного электроснабжения в филиале банка используется источник бесперебойного питания APC by Schneider Electric Back-UPS BK650EI (650 ВА) (производитель «APC by Schneider Electric», США).

Таким образом, организацию системы безопасности на исследуемом объекте следует признать удовлетворительной, однако в модернизации нуждается система контроля и управления доступом, которую необходимо интегрировать с имеющимися системами охранного видеонаблюдения, охранной и пожарной сигнализации.

3 Расчёты и аналитика

3.1 Выбор системы контроля и управления доступом

3.1.1. Общие принципы выбора СКУД

Выбор СКУД для объекта защиты осуществляется согласно рекомендациям Р. 78.36.005-2011 [6] и начинается с обследования объекта защиты. При обследовании определяются характеристики значимости помещений объекта, его строительные и архитектурно-планировочные решения, условия эксплуатации, режимы работы, ограничения (расширения) права доступа отдельных сотрудников, параметры установленных (или предполагаемых к установке на данном объекте) средств, входящих в СКУД. Цель предпроектного обследования состоит в определении комплекса мероприятий и разработке технических предложений с учетом сформированных типовых решений. По результатам обследования составляется техническое задание на оборудование объекта СКУД. В техническом задании указывается назначение СКУД, техническое обоснование и описание системы, размещение составных частей системы, условия эксплуатации средств КУД. Прописываются основные технические характеристики СКУД.

Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, заземление составных частей системы и т.п. В помещении банка вредное воздействие окружающей среды следует учитывать для средств КУД входной двери. Особых условий (запыленность, повышенная влажность, отрицательная температура, агрессивная среда и т.п.) на объекте нет.

Выбор варианта СКУД неразрывно связан с требованиями обеспечения безопасности конкретного объекта. Зарубежный и отечественный опыт создания интегрированных систем безопасности показывает [29], что наиболее рациональным является реализация их «интеллектуального ядра» на базе

аппаратно-программных средств СКУД. Такой подход, в частности, позволяет сэкономить на аппаратуре СКУД и средствах охранной сигнализации (например, одни и те же дверные датчики положения могут применяться и в аппаратуре контроля доступа, и в охранной сигнализации).

Отечественные разработки СКУД более предпочтительны, даже если обладают худшими параметрами относительно зарубежных аналогов. Это объясняется невозможностью проанализировать математическое и программное обеспечение импортных СКУД. В условиях, когда СКУД определяет уровень безопасности объекта, «цена» каждого отказа и даже простого сбоя в работе аппаратуры слишком велика.

СКУД могут быть автономными и сетевыми. Выбор варианта зависит от цели монтажа и типа объекта. Если нужно только контролировать вход на охраняемую территорию, а аналитическая информация не имеет значения, выбирают автономную. Согласно Р 78.36.005-2011 [6] для объектов банковских структур выбирают многофункциональные сетевые СКУД.

Проведём сравнительный анализ некоторых имеющихся на рынке СКУД предложений, отмеченных в п. 1.4 в качестве наиболее востребованных потребителями.

3.1.2 Сравнительный анализ СКУД различных производителей

Определим оптимальный вариант СКУД для объекта банковской сферы с контролем восьми точек доступа и восьми сотрудников, для которых необходим учёт рабочего времени.

Основными критериями для выбора производителя были выбраны (приоритетность в порядке убывания):

- надёжность системы;
- удобство установки и эксплуатации;
- стоимость комплекта оборудования, монтажа и эксплуатации;
- возможность расширения системы с минимальными затратами.

Вопрос надежности СКУД требует отдельного исследования, поэтому ограничимся общими сведениями. Все цены взяты с официальных сайтов производителей и в большинстве зависят от курса валюты. Приведённые данные соответствуют апрелю 2020 г.

Проведём ценовое сравнение систем разных производителей. Учитывая довольно большой выбор на рынке СКУД, воспользуемся данными анализа, проведённого в [30] для 10 точек доступа (рис. 20).

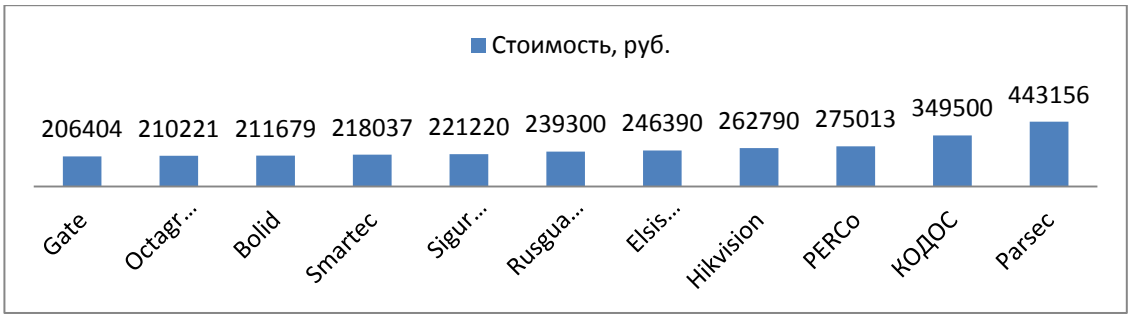


Рисунок 20 – Сравнение стоимости СКУД разных производителей

Рис. 20 показывает, что рассмариваемых производителей условно можно разделить на триценовые категории: «эконом» (Gate, Octagram, Bolid, Smartec и Sigur), средняя (Rusguard, Elsys, Hikvision и PERCo) и дорогие решения (КОДОС и Parsec). Однако стоит учитывать, что средний срок эксплуатации СКУД составляет около восьми лет, и, например, при покупке СКУД Smartec придется семь лет оплачивать услуги техподдержки. В этом случае данное решение переходит в категорию средних или дорогих. Учитывая этот факт, рассмотрим данные по СКУД среднего ценового диапазона и рассчитаем стоимость основного оборудования комплекта СКУД.

Для СКУД Elsys с ПО «Бастион» (ООО «ЕС-пром», г. Самара) выберем контроллер Elsys-MB-SM-2A-ТП с возможностью подключения двух считывателей на одну точку доступа и интерфейсом связи RS485. Для вывода в сеть всей группы контроллеров применяется коммуникационный контроллер Elsys-MB-Net. В связи с неблагополучной ситуацией по коронавирусной инфекции COVID-2019 турникет с пирометром. В линейке производителя имеется несколько различных считывателей, нас интересуют Smart-wave. Из программного обеспечения нам необходимы: лицензия на сервер системы,

модуль интеграции СКУД Elsys, модуль для учета рабочего времени «Бастион-2-АРМ УРВ Про» (табл. 4).

Таблица 4 – Перечень компонентов СКУД Elsys

Оборудование	Количество, шт.	Цена, руб.	Стоимость, руб.
Сетевой контроллер Elsys-MB-SM-2A-ТП	8	10350	82800
Коммуникационный контроллер Elsys-MB-Net	1	25730	25730
Считыватель proximity-карт Smart-wave	10	3030	30300
Турникет с пирометром	1	86270	86270
Лицензия на сервер системы АПК «Бастион» (не более 500 карт доступа)	1	12640	12640
Модуль интеграции СКУД Elsys	1	10070	10070
«Бастион-2-АРМ УРВ Про». Лицензия для одного АРМ	1	28030	28030
Итого			275840

Плюсом выбора решения данного производителя является возможность построения комплексных систем безопасности, не ограничиваясь только СКУД, довольно широкий ассортимент продукции. Однако следует отметить высокую стоимость коммуникационного контроллера и лицензии для учета рабочего времени.

Проанализируем оборудование компании «РусГард» (бренд RusGuard). Компания предоставляет клиентам бесплатное программное обеспечение [43].Для построения системы выбираем контроллер сетевой ACS-102-CE-BM, который предназначен для контроля одной двери в двухстороннем направлении. В паспорте на контроллер производитель указывает средний срок службы контроллера – 10 лет, однако эта модификация контроллера появилась в 2012 г., т.е. 7 лет назад. Считыватели применяем RDR-102-EH. Программное обеспечение RusGuard Soft единственное и включает в себя все необходимые нам модули. Турникет – трипод модели OxGuardPraktika, без встроенного пирометра. Пирометры на рынке имеют среднюю стоимость в пределах 3000–6000 руб. (табл. 5).

Таблица 5 – Перечень компонентов СКУД RusGuard

Оборудование	Количество, шт.	Цена, руб.	Стоимость, руб.
Сетевой контроллер в металлическом корпусе с блоком питания ACS-102-CE-BM	8	17390	139120
Считыватель универсальный RDR-102-EH	10	2940	29400
Турникет OxGuard Praktika	1	50847	50847
Пирометр Мегеон 16350	1	3150	3150
Программное обеспечение RusGuard Soft с неограниченным числом пользователей	1	бесплатно	бесплатно
Итого			222517

Довольно короткая спецификация упрощает монтаж, также положительным является бесплатный полный пакет ПО (единственный платный модуль – это создание шаблонов пропусков, который для нашей задачи не требуется). Тем не менее итоговая стоимость не самая низкая, кроме того информация на официальном сайте производителя противоречива.

Крупнейший производитель оборудования СКУД – компания PERCo (г. Санкт-Петербург) [10]. В арсенале данного производителя имеется универсальный контроллер, удовлетворяющий всем нашим требованиям, PERCo-CT/L04 (табл. 6). Считыватели PERCo-IR03 подключаются к контроллеру по интерфейсу RS485. Если применять считыватели с интерфейсом Wiegand, то потребуются преобразователи интерфейсов PERCo-AC02, стоимость которого около 3000 руб. Собственный резервный блок питания компания не производит, будем использовать источник известного производителя «Бастион» СКАТ-1200Д. Программное обеспечение имеет модульную структуру: выбираем модули: «Базовое ПО», «Администратор», «Персонал», «Управление доступом» и «Учет рабочего времени» комплексной системы безопасности. Оборудование этого производителя отличается большой и настраиваемой памятью контроллера, широким ассортиментом исполнительных устройств. Однако модульная политика лицензирования софта

вызывает значительное удорожание программного обеспечения, а отсутствие в линейке собственного резервного блока питания вызывает необходимость дополнительных поисков оборудования.

Таблица 6 – Перечень компонентов СКУД PERCo

Оборудование	Количество, шт.	Цена, руб.	Стоимость, руб.
Контроллер универсальный PERCo-CT/L04 на два считывателя	5	19060	95300
Считыватель PERCo-IR03	10	4393	43930
Преобразователи интерфейсов PERCo-AC02	5	2912	14560
Турникет PERCo-TTD-03.2G с функцией тепловизора	1	134296	134296
Программное обеспечение PERCo-SN-01 «Базовое ПО»	1	9211	9211
Сетевой модуль SM-01 «Администратор»	1	16317	16317
Сетевой модуль SM-02 «Персонал»	1	6428	6428
Сетевой модуль SM-04 «Управление доступом»	1	8759	8759
Сетевой модуль SM-07 «Учёт рабочего времени»	1	20832	20832
Источник вторичного питания резервированный 12 В, 2,3 А СКАТ-1200Д	5	2400	12000
Итого			361633

Hikvision – один из ведущих мировых производителей оборудования систем безопасности. Для решения нашей задачи подходят контроллеры DS-K2802 (на две двери и 4 считывателя) [31]. Блок питания DS-KAW50-1 выдает 4,2 А, что позволяет использовать также как и контроллер, один источник на две двери. Необходимо применять стороннее программное обеспечение, например «Интеллект» от компании ITV: «Ядро системы», «Интеграция с контроллерами СКУД Hikvision» и модуль учета рабочего времени. Компания Hikvision предлагает актуальное в современных условиях решение: терминал доступа с модулем определения повышенной температуры тела человека DS-K5604A-3XF/V (рис. 21). Кроме того, терминалом осуществляется детекция наличия или отсутствия маски.

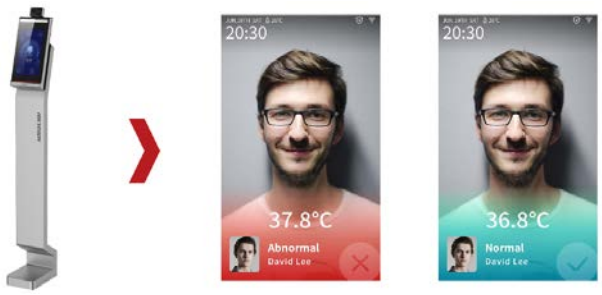


Рисунок 21 – Терминал доступа DS-K5604A-3XF/V

Положительной стороной решения контроля доступа HikVision является известность мирового бренда, широкий выбор оборудования, отрицательной стороной – необходимость использовать софт сторонних производителей, а также тот факт, что политика лицензирования ПО подразумевает оплату за каждый контроллер.

При выборе СКУД заказчику необходимо минимизировать риск выбора недобросовестного подрядчика. Тендеры не всегда являются оптимальным вариантом выбора, т.к. определяющим критерием является стоимость. Поэтому нами была проведена комплексная оценка подрядчиков, результаты которой были представлены в табл. 7.

Таблица 7 – Результаты сравнительной оценки подрядчиков

Критерий оценки	ООО «ЕС-пром», РФ	АО «РусГард», РФ	ООО «PERCo», РФ	HikVision, Китай
Контакты	Да	Да	Да	Да
Скорость реагирования	Автоматически	По запросу	По запросу	По запросу
Уставной капитал	50000 руб.	50000 руб.	254600000 руб.	–
Год регистрации	2011	2010	1988	2001, в РФ – 2009
Наличие реализованных проектов в банковской сфере	Да	Да	Да	Не показано
Наличие собственного штата монтажников	Да	Нет	Да	Нет
Он-лайн расчёт стоимости	Да	Да	Нет	Нет

С учётом предпринятого нами анализа по совокупности достоинств и недостатков выбираем решение СКУД Elsys с ПО «Бастион» компании ООО «ЕС-пром» (г. Самара).

3.2 Техническое задание на проектирование СКУД

3.2.1 Общее представление о техническом задании

Проектирование СКУД осуществляется в соответствии с Постановлением Правительства РФ от 16.02.2008 г. № 87 «О составе разделов проектной документации и требованиями к их содержанию» [32]. При проектировании СКУД учитываются требования существующего законодательства и нормативных документов по экологии, охране труда и пожарной безопасности:

- ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» [1];
- ГОСТ Р. 54831-2011 «Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний» [33];
- ПУЭ «Правила устройства электроустановок» [24];
- РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств» [19];
- Р 78.36.005-2011 «Выбор и применение систем контроля и управления доступом» [6];
- СТО НОСТРОЙ 2.15.10-2011 «Инженерные сети зданий и сооружений внутренние. Системы охранно-пожарной сигнализации, системы оповещения и управления эвакуацией, системы контроля и управления доступом, системы охранные телевизионные. Монтажные, пусконаладочные работы и сдача в эксплуатацию» [34].

Требования заказчика составляют основу технического задания на создание СКУД и являются документом, с которого начинается работа по созданию СКУД. Кроме технических требований, на первых этапах работы по проектированию СКУД в качестве исходной информации используются данные, полученные в процессе предпроектного обследования. От грамотного подхода к техническому заданию зависят сроки проектирования и выбор необходимого оборудования для СКУД.

3.2.2 Описание требований к компонентам СКУД

СКУД состоит из программной и технической части. Программная часть включает в себя следующие компоненты:

- комплект серверного и пользовательского программного обеспечения;
- комплект средств для обеспечения интеграции системы СКУД с другими системами безопасности банка.

Техническая часть включает: контроллеры СКУД; идентификаторы; считыватели и др.

Обработка информации происходит на центральном сервере с установленным серверным программным обеспечением. Взаимодействие устройств СКУД осуществляется по определённым каналам связи: Ethernet, RS485. СКУД должна обслуживать следующие помещения и устройства по типам: двери помещений; турникет. Проход через турникет осуществляется с видеоверификацией проходящего через устройство человека посредством IP-камеры и контролем температуры. Вывод изображения осуществляется на АРМ сотрудника охраны и передаётся на сервер, где сохраняется. При запуске системы оповещения о пожаре турникет автоматически открывается.

Входная дверь, оборудованная врезным сдвиговым электромагнитным замком типа AL-300, в рабочее время постоянно открыта, в нерабочее – находится под охраной ФГУП «Охрана» Росгвардии.

Для служебных помещений, помимо функций контроля доступа, система должна поддерживать выполнение охранных функций, то есть постановку и снятие помещения из-под охраны картой доступа. Каждое контролируемое помещение быть оборудовано светозвуковым устройством, отражающим текущее состояние помещения. Светозвуковое устройство выполнено в едином корпусе со считывателем. На случай нештатной блокировки дверей, внутри каждого помещения устанавливается кнопка принудительного открывания. При запуске системы оповещения о пожаре двери всех контролируемых помещений, находящиеся не под охраной, должны перейти в открытое состояние.

3.2.3 Алгоритмы работы СКУД в отдельных помещениях

Алгоритм работы системы для входной двери: в штатном режиме входная дверь находится под охраной. Вход первого имеющего доступ работника в считается снятием помещения с охраны. При снятии с охраны система обесточивает врезной сдвиговый электромагнитный замок. В конце рабочего дня последний уходящий сотрудник (сотрудник охраны) ставит входную дверь на охрану. Этапы постановки помещения под охрану должны отражаться состоянием светозвукового устройства.

Алгоритм работы системы для служебных помещений: в дежурном режиме служебные помещения стоят под охраной. На АРМ отображается планировка всех помещений банка с текущим состоянием всех шлейфов. В случае несанкционированного проникновения на мониторе появляется планировка здания и сработавший шлейф. Ведется журнал учета сработок.

В соответствии с режимом работы банка, за 10 мин до установленного времени открытия, для конкретного работника активируется доступ к конкретному помещению. При снятии с охраны помещения путём идентификации карты доступа считывателем, система обесточивает врезной сдвиговый электромагнитный замок. В неохраняемый период контроллер помещения выполняет функцию регистратора присутствующих. Каждый

входящий через считыватель регистрирует свое присутствие путём прикладывания к считывателю персональной карты. В конце рабочего дня работник прикладывает персональную карту к считывателю-регистратору, дверной замок переходит в закрытое состояние. Этапы постановки помещения под охрану должны отражаться состоянием светозвукового устройства. В случае неудачной постановки на охрану, система посылает повторный запрос на постановку и лишь потом отправляет сигнал ошибки на АРМ охраны.

Алгоритм работы системы для дверей бытовой комнаты: контроль открывания таких дверей предполагает проход через них по реакции входного считывателя на права доступа пользователя.

3.2.4 Работа СКУД при изменении условий функционирования

Программное обеспечение СКУД должно обеспечивать возможность дальнейшего расширения системы (количества контроллеров, пользователей в системе, количества удалённых рабочих мест). Система должна сохранять работоспособность и обеспечивать восстановление своих функций (при перезапуске) при возникновении следующих внештатных ситуаций:

- при сбоях в работе аппаратной части, приводящих к перезагрузке операционной системы сервера СКУД;
- при ошибках в работе программного обеспечения СКУД;
- при ошибках, связанных с программным обеспечением сторонних производителей (например, драйверов устройств), восстановление работоспособности возлагается на операционную систему сервера СКУД.

3.2.5 Требования к контроллерам СКУД

Контроллеры СКУД устанавливаются внутри охраняемого (защищаемого) объекта и обеспечивают круглосуточный режим работы. Согласно ГОСТ Р 51241-2008 [1] средняя наработка контроллеров СКУД на

отказ должна составлять не менее 10 000 ч, средний срок службы контроллеров СКУД должен быть не менее 8 лет с учетом проведения восстановительных работ. Система электропитания контроллеров СКУД обеспечивает защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение и автоматическое восстановление электропитания после устранения причины неисправности. Конструкция контроллеров СКУД должна обеспечивать пожарную безопасность в аварийном режиме работы и при нарушении правил эксплуатации согласно ГОСТ 12.1.004-91 [35]. Факторы, оказывающие вредные воздействия на здоровье, связанные с работой контроллеров СКУД не должны превышать действующих норм СанПиН 2.2.2./2.4.1340-03 [36]. Конструкция контроллеров СКУД должна обеспечивать степень защиты оболочки IP20 по ГОСТ 14254-2015 [37]. Контроллеры должны сохранять работоспособность и выполнение всех предъявляемых требований при воздействии внешних электромагнитных помех. Контроллеры СКУД должны быть универсальными и поддерживать сразу несколько типов точек доступа: двери, турникет и др.

Контроллеры должны аппаратно поддерживать режим глобального AntiPassBack без участия сервера, т.е. запрет двойного прохода – предотвращать проход двух и более посетителей по одному идентификатору, формировать точные отчеты рабочего времени сотрудников предприятия.

Контроллеры должны поддерживать работу со считывателями форматов Wiegand-26 и TouchMemory. На контроллере должна быть предусмотрена возможность совместимости со считывателями разных производителей.

3.2.6 Требования к программному обеспечению СКУД

Программная часть СКУД должна обеспечивать защиту от несанкционированного доступа. Уровень защиты информации определяется согласно приказу Федеральной службы РФ по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении требований о защите

информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [38]. Класс защищенности информационной системы объекта защиты определяется в зависимости от уровня значимости обрабатываемой информации и масштаба информационной системы.

Учитывая, что филиал ПАО КБ «Восточный» является частью информационной системы, функционирующей на территории Российской Федерации, т.е. имеет федеральный масштаб, определим уровень защиты информации как 1Д по классификации РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем» [39]. Согласно этому защита от несанкционированного доступа должна проводиться по трём направлениям:

- идентификация пользователя;
- проверка полномочий пользователя при работе с системой;
- разграничение доступа пользователей.

Программное обеспечение СКУД должно восстанавливать свое функционирование при корректном перезапуске аппаратных средств. Должна быть предусмотрена возможность организации автоматического и (или) ручного резервного копирования данных системы.

3.2.7 Требования к монтажу СКУД

Все работы выполняются в соответствии с действующим законодательством РФ с обязательным выполнением норм и правил охраны труда, пожарной безопасности и техники безопасности, производственной санитарии, учитывая специфику здания и соблюдением внутреннего распорядка нахождения на охраняемой территории (соблюдать режимные требования и пропускной режим, установленные на объекте).

При проводке кабельных линий не повреждать технические и инженерные коммуникации, предотвратить доступ к ним посторонних лиц.

Работы выполнять согласно разработанному и утвержденному Заказчиком сметному расчету, при составлении сметной документации применять расценки на материалы и виды работ по Федеральным единичным расценкам ФЕР-2020, утверждёнными приказом Минстроя РФ № 876 от 26.12.2019 г. [40].

Подрядчик должен гарантировать качество выполненных работ и используемых материалов, гарантийный срок качества выполненных работ с момента сдачи работ должен составлять не менее 12 месяцев.

Грамотно разработанная концепция СКУД и техническое задание дает основания для создания проекта СКУД – единого комплекса решений, предназначенного для обеспечения заданного режима эксплуатации СКУД. Проект определяет оптимальную структуру СКУД и трассу прокладки кабельных проводок, расположение и состав элементов СКУД. Проектная документация СКУД представляет собой текстовые и графические материалы, определяющие объемно-планировочные, конструктивные и технические решения для строительства СКУД. Она обеспечивает детальную привязку компонентов СКУД к объекту и содержит чертежи, таблицы соединений и подключений, планы расположения оборудования и проводок и другие документы.

3.3 Проект СКУД филиала ПАО КБ «Восточный» в г. Юрга

3.3.1 Описание проектного решения

3.3.1.1 Компонентный состав СКУД филиала ПАО КБ «Восточный» в г. Юрга

Решение СКУД разработано на основе типового проекта, размещённого на сайте производителя и обеспечивает:

- санкционированный доступ сотрудников в зоны и выделенные помещения;

- выдачу сигнала тревоги на АРМ дежурного оператора или на пульт управления в случае несанкционированного доступа (открытия двери) в зоны доступа и выделенные помещения;

- компьютерный учет входа и выхода посетителей и сотрудников с ведением протокола в компьютере и вывода протокола на принтер;

- контроль и регистрацию перемещения персонала в протоколе компьютера;

- возможность временного блокирования дверей, не участвующих в обеспечении технологического цикла.

В состав СКУД входят:

- станционное оборудование, в состав которого входят сервер ELSYS Бастион-2-Сервер 5000 и АРМ сотрудника охраны «Бастион-2-АРМ УРВ Про», реализованные на базе персональных компьютеров, объединенные в локальную сеть, сетевой коммутатор Elsys-MB-Net;

- линейное оборудование, включающее в себя контроллеры СКУД Elsys-MB-SM-2A-ТП. Контроллеры соединены между собой двухпроводной линией связи с интерфейсом RS-485 по схеме общей шины. В качестве среды передачи данных интерфейса RS-485 используются медные витые пары. Эти группы контроллеров подключены к серверу, с которого осуществляется управление и программирование каждого контроллера;

- абонентские устройства: электромеханический турникет-трипод с контролем температуры тела Elsys ST-TS100, электромагнитные замки «ML-200 M», считыватели бесконтактных карт доступа Smart-wave, кнопки «ВЫХОД» и кнопки разблокировки замков (турникета) в случае возникновения чрезвычайной ситуации, магнитоконтактные извещатели «ИО 102-16/2», видеодомофон «VideoNova A40-IP-16». В Приложении А показана общая схема помещения, а в Приложении Б – план расположения оборудования и кабельных трасс.

В состав СКУД входят точки контроля доступа (ТКД) двух типов: двери одно- или двухсторонние – в помещения банка; турникет – вход в здание. Точка

контроля доступа функционально состоит из контроллера доступа, исполнительного механизма (турникет, дверь), считывателей, магнитоконтактных извещателей. В состав ТКД входит источник резервированного питания для поддержания работоспособности устройств при временном пропадании напряжения питающей сети.

Проход через точки с контролем доступа осуществляется при поднесении бесконтактной карты к считывателю. В случае успешной идентификации карты доступа системой исполнительное устройство разблокируется, разрешая однократный проход. Каждой карте в базе данных СКУД присваиваются определенные права доступа и сведения: список разрешенных точек входа; расписание разрешенного прохода; данные по сотруднику (Ф.И.О., должность и т.д.); фотография сотрудника; табельный номер; дополнительные параметры (при необходимости). Каждая точка прохода контролируемая системой, может быть открыта для прохода различными способами:

- автоматический (по предъявлению бесконтактной карты считывателю)

- пропуск постоянных сотрудников, идущих без нарушений временного режима и зоны доступа;

- прямая команда с АРМ в случае необходимости свободного доступа или доступа по разовым пропускам;

- централизованное отключение запирающих устройств на всех точках прохода, применяемое в экстренных ситуациях, связанных с природными катаклизмами, пожаром и т.п.

- ручное управление с кнопок разблокировки.

Любой из названных способов открытия точки прохода фиксируется в протоколе системы. Протокол хранится на жестком диске сервера СКУД, доступ к протоколу защищен паролем.

Управление системой и мониторинг за её работой осуществляется с сервера и с АРМ оператора. Сервер представляет собой высокопроизводительный компьютер. Контроллеры доступа подключаются к серверу посредством преобразователя интерфейсов USB/RS-485. Сервер

работает под управлением операционной системы Windows 10 и программного комплекса «Бастион» с драйверами оборудования «Бастион-Elsys». Дополнительно на сервер устанавливается программный модуль «Бастион-Архив», который позволяет осуществлять администрирование базы данных протокола (создавать резервные копии, производить очистку или выгрузку данных протокола).

Автоматизированное рабочее место представляет собой персональный компьютер, работающий под управлением операционной системы Windows 10 и программного модуля «Бастион-Сеть». С АРМ осуществляется контроль, управление и настройка оборудования. Сервер и АРМ объединяются в локальную сеть посредством сетевого коммутатора.

Двухсторонним доступом оборудуются помещения кассы и руководителя. В этом случае считыватели устанавливаются с обеих сторон двери. С внутренней стороны дополнительно устанавливается кнопка пожарной разблокировки. Размещение оборудования двери с двусторонним доступом показано в Приложении В. При возникновении экстренной ситуации дверь может быть разблокирована изнутри кнопкой разблокировки. При этом событие «Ручная разблокировка двери» фиксируется в протоколе событий системы.

С внешней стороны двери, оборудованной односторонним доступом (Приложение Г), устанавливается считыватель бесконтактных идентификационных карт доступа, а с внутренней стороны – кнопка выхода. Блокировка двери осуществляется электромеханическим замком, устанавливаемым в косяк. Закрывание двери обеспечивает гидравлический доводчик. Контроллер управления дверью устанавливается в непосредственной близости от точки доступа. Проход через точку доступа осуществляется следующим образом: сотрудник или посетитель, предоставляет карту доступа бесконтактному считывателю, установленному рядом с контролируемой дверью. При успешной идентификации (наличии прав доступа в соответствующую зону контроля) дверь разблокируется, позволяя осуществить

однократный вход (о результате идентификации сигнализирует сам считыватель светозвуковым и звуковым оповещением). Для выхода из контролируемой зоны сотрудник или посетитель должны нажать кнопку выхода, при этом дверь разблокируется, позволяя осуществить однократный выход.

В холле расположен турникет для прохода постоянных сотрудников и клиентов банка. Проектным решение предполагается установка одного турникета для беспрепятственного и своевременного прохода сотрудников и посетителей. Вывод сделан на основе данных наблюдений за количеством посещений банка. Наблюдения проводились в течение 6 рабочих дней в течение всего дня. Данные наблюдений приведены в табл. 8. Учитывая, что количество персонала составляет 8 чел, а пропускная способность турникета 15 чел./мин, будем считать только посетителей.

В ходе наблюдений установлено, что пропускная способность одного турникета значительно превышает количество людей, находящихся в помещении банка. Анализируя полученные результаты, можно сделать вывод, что достаточно установить один турникет.

Таблица 8 – Количество посетителей филиала ПАО КБ «Восточный»

Период	Понедельник	Вторник	Среда	Четверг	Пятница	Суббота
09.00–10.00	4	5	2	4	2	–
10.00–11.00	6	4	2	6	1	7
11.00–12.00	6	6	1	8	1	5
12.00–13.00	3	5	7	2	0	8
13.00–14.00	7	3	6	3	8	2
14.00–15.00	2	1	3	3	9	2
15.00–16.00	6	0	8	7	6	1
16.00–17.00	6	6	2	7	3	0

В приложении Д приведена структурная схема СКУД. Размещение оборудования СКУД по точкам доступа представлено в табл. 9.

Таблица 9 – Размещение оборудования СКУД

Точка доступа	Расположение	Оборудование
ТД1	Помещение кредитного эксперта	Контроллер Elsys-MB-SM-2A-ТП, считыватель Elsys-SW10-EH, магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери без фиксации, замок электромагнитный «ML-200 M»
ТД2	Помещение кредитного эксперта	Считыватель Elsys-SW10-EH, магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери без фиксации, замок электромагнитный «ML-200 M»
ТД3	Кабинет управляющего	Контроллер Elsys-MB-SM-2A-ТП, коммутатор Elsys-MB-Net, сервер IBM, считыватель Elsys-SW10-EH – 2 шт., магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери с фиксацией, замок электромагнитный «ML-200 M»
ТД4	Бытовое помещение	Контроллер Elsys-MB-SM-2A-ТП, считыватель Elsys-SW10-EH, магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери без фиксации, замок электромагнитный «ML-200 M»
ТД5	Служебный вход в кассу	Контроллер Elsys-MB-SM-2A-ТП, считыватель Elsys-SW10-EH, магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери без фиксации, замок электромагнитный «ML-200 M»
ТД6	Касса	Контроллер Elsys-MB-SM-2A-ТП, считыватель Elsys-SW10-EH – 2 шт., магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери с фиксацией, замок электромагнитный «ML-200 M»
ТД7	Вход для посетителей в кассу	Контроллер Elsys-MB-SM-2A-ТП, считыватель Elsys-SW10-EH, магнитоконтактный извещатель «ИО 102-16/2», кнопка открытия двери без фиксации, замок электромагнитный «ML-200 M»
ТД8	Вход в здание	Контроллер Elsys-MB-SM-2A-ТП, АРМ, видеомагнитофон «VideoNova A40-IP-16», турникет Elsys ST-TS100, замок электромеханический

Таким образом, проектное решение обеспечивает все восемь точек доступа средствами КУД.

3.3.1.2 Электроснабжение СКУД филиала ПАО КБ «Восточный» в г. Юрга

Питание СКУД осуществляется от сети переменного напряжения 220 В, 50 Гц. Защита подводящего кабеля осуществляется автоматическими

выключателями. Оборудование, входящее в состав СКУД заземляется согласно ПУЭ [24].

Рассчитаем токи потребления системы контроля и управления доступом. При отключении централизованного электроснабжения источники бесперебойного питания обеспечивают нормальную работу системы контроля и управления доступом в течение 1 ч. В табл. 10–17 представлены результаты расчётов по подбору источников бесперебойного питания для точек доступа.

Учтем, что номинальная мощность источника бесперебойного питания должна быть на 25% больше, чем мощность нагрузки.

Таблица 10 – Оборудование кабинета управляющего (ТД3)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования, шт.	Сумма, Вт
Компьютер-сервер	300	1	300
Монитор	40	1	40
Коммутатор	20	1	20
Контроллер	250	1	250
Считыватель	1,2	2	2,4
Магнитоконтактный извещатель	10	1	10
Замок электромагнитный	6	1	6
		Итого	628,4

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания POWERMAN ONLINE 1000 Plus мощностью 800 Вт.

Таблица 11 – Оборудование кабинетов кредитных экспертов (ТД1, ТД2)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма, Вт
Считыватель	20	2	40
Контроллер	250	1	250
Магнитоконтактный извещатель	10	2	20
Кнопка открытия двери без фиксации	10	2	20
Замок электромагнитный	6	2	12
		Итого	342

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания CyberPower BS450E мощностью 425 Вт.

Таблица 12 – Оборудование бытового помещения (ТД4)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма, Вт
Считыватель	20	1	20
Контроллер	250	1	250
Магнитоконтактный извещатель	10	1	10
Кнопка открытия двери без фиксации	10	1	10
Замок электромагнитный	6	1	6
		Итого	296

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания APC BK650EI Back-UPS CS мощностью 400 Вт.

Таблица 13 – Оборудование служебного входа в кассу (ТД5)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма,Вт
Считыватель	20	1	20
Контроллер	250	1	250
Магнитоконтактный извещатель	10	1	10
Кнопка открытия двери без фиксации	10	1	10
Замок электромагнитный	6	1	6
		Итого	296

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания APC BK650EI Back-UPS CS мощностью 400 Вт.

Таблица 14 – Оборудование кассы (ТД6)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма, Вт
Считыватель	20	2	40
Контроллер	250	1	250
Магнитоконтактный извещатель	10	1	10
Кнопка открытия двери с фиксацией	10	1	10
Замок электромагнитный	6	1	6
		Итого	316

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания APC BK650EI Back-UPS CS мощностью 400 Вт.

Таблица 15 – Оборудование входа для посетителей кассы (ТД7)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма, Вт
Считыватель	20	1	20
Контроллер	250	1	250
Магнитоконтактный извещатель	10	1	10
Кнопка открытия двери без фиксации	10	1	12
Замок электромагнитный	6	1	12
		Итого	304

Для резервирования системы по питанию на 1 ч установим источник бесперебойного питания APC BK650EI Back-UPS CS мощностью 400 Вт.

Таблица 16 – Оборудование входа в здание отделение банка (ТД8)

Наименование оборудования	Потребляемая мощность, Вт	Количество оборудования	Сумма, Вт
Видеомагнитофон	20	1	20
Контроллер	250	1	250
Турникет	60	1	60
Замок электромагнитный	6	1	6
		Итого	336

Для резервирования системы по питанию на 1 ч необходимо установить источник бесперебойного питания CyberPower BS450E мощностью 425 Вт.

Расчет источника питания контроллеров приведен в таблице 17.

Таблица 17 – Расчёт источника питания контроллеров (ТД1, ТД2)

Наименование оборудования	Ток потребления, мА	Количество оборудования	Сумма, А
Контроллер	250	1	0,25
Считыватель	50	2	0,1
Замок электромагнитный	350	2	0,7
		Итого	1,05

Для расчета источника питания контроллеров выберем максимально нагруженный контроллер Elsys-MB-Light, управляющий двумя точками доступа (ТД1, ТД2). Рассчитаем необходимую ёмкость батареи на 1 ч, взяв коэффициент запаса, равный 1,3:

1,05 А × 1 ч × 1,3 = 1,365 А·ч.

Для питания контроллера и подключенных к нему исполнительных устройств использовать источник питания Elsys-SWPS-2A с номинальным током потребления 2 А. Для обеспечения бесперебойной работы контроллеров при отключении централизованного электроснабжения подключаем к источнику питания аккумулятор 12 В, 7 А·ч.

3.3.1.3 Требования к монтажу оборудования и прокладке кабельных трасс

Контроллеры СКУД устанавливают в непосредственной близости от точек прохода в недоступном для посторонних лиц месте. Крепление производят саморезами и пластиковыми дюбелями. Пульт управления турникетом устанавливают на стол рабочего места поста охраны. Турникет устанавливают согласно инструкции по эксплуатации на бетонную поверхность. Провода к турникетам подводят в гофрированных трубах под поверхностью пола в штробах согласно инструкции по эксплуатации. Считыватель устанавливают на привод турникета в соответствии с техническими условиями.

Считыватели, контролирующие проход через двери устанавливают на уровне 1,2 м от уровня пола, согласно схемам установки оборудования дверей и инструкции по эксплуатации. Электромагнитные замки, доводчики устанавливают согласно инструкции по эксплуатации и чертежам производителя. Линии связи выполняют выполняют кабелем КВП-5е 4×2×0,52 при внутренней прокладке и кабелем КВПВП-5е 4×2×0,52 при уличной прокладке. Линии связи линейного оборудования устанавливают проводами КВП-5е 4×2×0,52 и КСПВГ 4×0,2 в соответствии со схемами подключения

контроллеров. Подвод сетевого питания к автоматам питания СКУД осуществляют в соответствии с ПУЭ [24], обеспечивая необходимое заземление или зануление питающей сети. Электропитание подводят к аппаратуре кабелями ПБОВ 3×1 в соответствии с техническими описаниями устройств. Соединение узлов системы производят в соответствии со схемами подключения и технической документацией изготовителей.

3.3.1.4 Технические характеристики основных узлов системы

Для построения СКУД используются контроллеры «Elsys-MB-SM-2A-ТП» (производитель – ООО «НИЦ «ФОРС»), предназначенные для работы в составе интегрированной системы контроля и управления доступом. Применяется для организации работы точки доступа. Имеет в своем составе источник бесперебойного питания, модуль расширения памяти, сетевой трансформатор. Допускает круглосуточное функционирование в течение всего срока эксплуатации. Основные технические характеристики:

- количество управляемых турникетов – 1;
- количество подключаемых считывателей – 2;
- количество событий в памяти – 3500;
- тип используемой линии связи – RS-485;
- максимальная длина линии связи – 1200 м;
- максимальное количество контроллеров в линии связи – 32;
- напряжение питания – 220±22 В;
- ток потребления – не более 300 мА;
- материал корпуса – металл.

Proximity считыватель Smart-wave (производитель – ООО «НИЦ «ФОРС») предназначен для использования в системах СКУД и ориентирован на применение интерфейсов Wiegand и Touch Memory. Считыватель используется с картами EM-Marin и HID. Основные технические характеристики:

- напряжение – 8–18 В;

- ток – 50мА;

- расстояние считывания – 60–140мм;

- рабочая температура – от минус 40 до плюс 40 °С.

Замок электромагнитный ML-200M применяется совместно с контроллерами доступа, допускает круглосуточное функционирование в течение всего срока эксплуатации. Основные технические характеристики:

- усилие блокировки – 200 кг;

- напряжение питания – 12 В;

- ток потребления – 350 мА;

- материал корпуса – металл.

Извещатель магнитоконтактный «ИО-102-16/2»предназначен для блокировки дверных проемов при несанкционированном открывании.Основные технические характеристики:

- тип контактов – нормально замкнутые;

- расстояние между магнитом и герконом при замыкании (размыкании) контактов – менее 10мм (более 45 мм);

- ток потребления – 250 мА;

- срок службы – $5 \cdot 10^5$срабатываний;

- масса – не более 0,015 кг;

- материал корпуса – полистирол.

3.3.1.5 Система тревожной сигнализации

Тревожная кнопка (извещатель охранный ручной) – комплекс охранных приборов**,** которые отправляют сигнал на пультовую охрану для немедленного выезда группы быстрого реагирования. Тревожные кнопки могут быть стационарными и переносными, которые представляют собой компактное мобильное устройство – брелок, который выдаётся сотрудникам. Для передачи сигнала используется сотовая связь или радиоканал. Стационарные кнопки

имеют несколько вариантов исполнения: стандартные (рис. 22), нажимные (педали), «куклы» (например, в виде пачки денежных купюр).

Рисунок 22 – Виды тревожных кнопок

В стандартный базовый комплект входят: тревожная кнопка стационарная, устройство приёмно-контрольное с GSM-коммуникатором и резервный источник питания. Кнопка может иметь ключ для блокировки кнопки в нажатом состоянии до приезда наряда. Схема подключения тревожной кнопки представлена на рис. 23. При нажатии на кнопку цепь размыкается, и ток идёт через сопротивление. Прибор это фиксирует и отправляет сигнал. Сопротивление необходимо для того, чтобы злоумышленники не смогли обойти кнопку и подключить шлейф напрямую. Монтируют сопротивление непосредственно возле кнопки или в её корпус.

а б

Рисунок 23 – Схема подключения тревожной кнопки:

а – общий вид; б – электрическая схема;

И1 – извещатель, ШС – шлейф сигнализации; $R_ш$ – резистор; $R_ок$ – оконечный резистор

Преимуществами кнопки тревожной сигнализации (КТС) являются простота монтажа, элементарное взаимодействие, быстрое реагирование, небольшая стоимость, чувство безопасности сотрудников. Однако пользоваться КТС нужно очень осторожно, не заметно для грабителей. Иногда бывают

случаи, когда лучше не прибегать к использованию тревожной кнопки, в целях собственной безопасности и безопасности других. Учитывая этот факт, а также особенности объекта защиты (денежные средства хранятся только в помещении кассы,), в качестве проектного решения предлагаем использовать извещатель охранный ручной точечный электроконтактный «КУКЛА-Л», предназначенный для организации охраны мест хранения наличных денежных средств путём формирования тревожных извещений при изменении положения закладного элемента, закамуфлированного в упаковке банкнот (рис. 24). Производитель – компания «Септима», г. Москва. Извещатель охранный «КУКЛА-Л» применяется для охраны мест хранения наличных денежных средств путем передачи тревожного сигнала на пульт в момент перемещения извещателя на расстояние более 10 мм. Конструкция извещателя, выполненная в виде пачки купюр объёмом 100 листов, позволяет ему не выделяться на фоне защищаемых денежных средств и предполагает его установку в сейфах, кассах, ящиках столов. Внутри находятся источник питания и контактная пара с чекой.

Рисунок 24 – Извещатель охранный ручной точечный электроконтактный «КУКЛА-Л»

При попытке изъятия ловушки с места установки произойдет удаление чеки из контактной пары и изделие срабатывает с выбросом несмываемой с кожи и одежды человека жидкостной красящей композиции ярко-малинового цвета на расстояние не менее 1,5 м и образованием аэрозольного облака слезоточивого действия. При установке извещателя следует учитывать направление выброса красящей композиции и слезоточивого состава, которые показаны стрелками на упаковке.

По данным экспертов [18], извещатели «КУКЛА-Л» довольно часто применяются в банковской сфере, помогая обезвреживать преступников в

экстренной ситуации. В последние годы усиливается интерес к извещателям подобного типа, увеличивается их ассортимент на рынке, т.к. предлагаемые извещатели довольно эффективны при простоте и невысокой стоимости.

3.4 Расчёт надёжности

ГОСТ 27.002-89 [52] указывает, что надежность – это свойство изделия (объекта) сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортирования. Согласно ГОСТ Р 51241-2008 [1] к СКУД устанавливаются следующие требования по надёжности: средняя наработка на отказ должна быть не менее 10000 ч (без учёта УПУ), средний срок службы – не менее восьми лет.

Будем считать, что СКУД работоспособна, когда работоспособны все ее элементы без исключения. Отказы отдельных элементов возникают по причинам их естественного старения и не зависят от состояний других элементов системы. Все структурные элементы в СКУД восстанавливаются. Случайные величины времени безотказной работы и времени восстановления всех элементов СКУД распределены по экспоненциальному закону. Все кабельные изделия считаются абсолютно надежными.

Определим надёжность системы контроля и управления доступом, состоящей из следующих компонентов (без учёта УПУ): контроллер Elsys-MB-SM-2A-ТП, коммутатор Elsys-MB-Net (таблица 18). В состав контроллера входят следующие узлы:

- стабилизатор напряжения 5 В;
- литиевая батарея номинальным напряжением 3 В;
- однокристальный микроконтроллер (далее – микропроцессор);
- часы реального времени;
- энергонезависимая память EEPROM;

- схема сопряжения с линией связи RS-485;

- входные цепи, согласующие входы контроллера с линиями микропроцессора;

- входные цепи, согласующие интерфейсные линии считывателей с линиями микропроцессора;

- выходные ключи, обеспечивающие согласование линий микропроцессора с выходами базового модуля контроллера;

- два реле,

- 9-элементный DIP-переключатель, используемый для установки адреса и скорости обмена информацией.

Стабилизатор напряжения согласно принципиальной электрической схеме является сложным прибором и содержит элементы, представленные в табл. 18. В расчёт надежности не включаем процессы соединений деталей (пайки).

Таблица 18 – Расчёт показателей надёжности стабилизатора напряжения

Наименование компонента	Количество компонентов, N_i	Интенсивность отказов, $ч^{-1}$		Вероятность безотказной работы, P(t)	Вероятность отказов, Q(t)
		$\lambda_i \cdot 10^6$	$N_i \lambda_i \cdot 10^6$		
Резистор	5	0,05	0,25	0,997	0,003
Операционный усилитель	1	1	1	0,99	0,01
Транзистор биполярный	1	0,3	0,3	0,997	0,003
Стабилитрон	1	0,2	0,2	0,998	0,002

$$\sum_{i=1}^{4} N_i = 8; \quad \lambda_c = \sum_{i=1}^{4} N_i \lambda_i = 1,7 \cdot 10^{-6} \text{ ч}^{-1}.$$

По данным таблицы 18 и по формуле для экспоненциального закона найдём вероятность безотказной работы стабилизатора напряжения в течение t = 10000 ч и среднюю наработку до первого отказа:

$$P_c(10000) = e^{-\lambda_c t} = e^{-1,7 \cdot 10^{-6} \cdot 10000} = 0,98,$$

$$t_{ср.с} = \frac{1}{\lambda_c} = \frac{1}{1,7 \cdot 10^{-6}} = 588235 \text{ ч} \approx 67 \text{ лет}.$$

Расчёт по отдельным компонентам даёт:

$$P_c(10000) = e^{-0,25\cdot10^{-6}\cdot10000} = 0,997,$$

$$P_c(10000) = e^{-1\cdot10^{-6}\cdot10000} = 0,99,$$

$$P_c(10000) = e^{-0,3\cdot10^{-6}\cdot10000} = 0,997,$$

$$P_c(10000) = e^{-0,2\cdot10^{-6}\cdot10000} = 0,998.$$

Расчёт надежности контроллера проведём согласно [42] и найдём вероятность безотказной работы системы в течение t = 10000 ч и среднюю наработку до первого отказа (табл. 19). В расчёте использовались справочные данные об интенсивности отказов комплектующих компонентов [43].

Таблица 19 – Расчёт показателей надёжности контроллера

Наименование компонента	Количество компонентов, N_i	Интенсивность отказов, $ч^{-1}$		Вероятность безотказной работы, P(t)	Вероятность отказов, Q(t)
		$\lambda_i \cdot 10^6$	$N_i \lambda_i \cdot 10^6$		
Стабилизатор напряжения 5 В	1	1,7	1,7	0,983	0,017
Литиевая батарея номинальным напряжением 3 В	1	0,22	0,22	0,998	0,02
Микропроцессор	1	0,23	0,23	0,998	0,002
Часы реального времени	1	0,02	0,02	0,9998	0,0002
Энергонезависимая память EEPROM	1	0,017	0,017	0,9998	0,0002
Реле	2	0,3	0,6	0,994	0,94
DIP-переключатель	1	0,14	0,14	0,999	0,001

$$\sum_{i=1}^{7} N_i = 8; \quad \lambda_c = \sum_{i=1}^{7} N_i \lambda_i = 2,9 \cdot 10^{-6} \text{ ч}^{-1}.$$

По данным таблицы 18 и по формуле для экспоненциального закона найдём вероятность безотказной работы контроллера в течение t = 10000 ч и среднюю наработку до первого отказа:

$$P_c(10000) = e^{-\lambda_c t} = e^{-2,9\cdot10^{-6}\cdot10000} = 0,97,$$

$$t_{ср.с} = \frac{1}{\lambda_c} = \frac{1}{2,9\cdot10^{-6}} = 344827 \text{ ч} \approx 39 \text{ лет}.$$

Расчёт по отдельным компонентам даёт:

$$P_c(10000) = e^{-1,7\cdot10^{-6}\cdot10000} = 0,983,$$

$$P_c(10000) = e^{-0,22\cdot10^{-6}\cdot10000} = 0,998,$$

$$P_c(10000) = e^{-0,23\cdot10^{-6}\cdot10000} = 0,998,$$

$$P_c(10000) = e^{-0,02\cdot10^{-6}\cdot10000} = 0,9998,$$

$$P_c(10000) = e^{-0,017\cdot10^{-6}\cdot10000} = 0,9998,$$

$$P_c(10000) = e^{-0,6\cdot10^{-6}\cdot10000} = 0,994,$$

$$P_c(10000) = e^{-0,14\cdot10^{-6}\cdot10000} = 0,999.$$

Определим вероятность безотказной работы СКУД в целом без учёта УПУ в течение t = 10000 ч и среднюю наработку до первого отказа:

Таблица 20 – Расчёт показателей надёжности СКУД

Наименование компонента	Количество компонентов, N_i	Интенсивность отказов, $ч^{-1}$	
		$\lambda_i \cdot 10^6$	$N_i \lambda_i \cdot 10^6$
Коммутатор	1	0,15	0,15
Контроллер	7	2,9	20,3

$$\sum_{i=1}^{2} N_i = 8; \quad \lambda_c = \sum_{i=1}^{2} N_i \lambda_i = 3,05 \cdot 10^{-6} \text{ ч}^{-1}.$$

По данным таблицы 18 и по формуле для экспоненциального закона найдём вероятность безотказной работы СКУД в течение t = 10000 ч и среднюю наработку до первого отказа:

$$P_c(10000) = e^{-\lambda_c t} = e^{-3,05\cdot10^{-6}\cdot10000} \approx 0,98,$$

$$t_{ср.с} = \frac{1}{\lambda_c} = \frac{1}{3,05\cdot10^{-6}} = 327869 \text{ ч} \approx 37 \text{ лет}.$$

Для более полной оценки надёжности рассчитаем коэффициент готовности СКУД – вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается, по формуле [42]:

$$K_Г = \frac{T}{T + T_в}, \quad (1)$$

где T – наработка на отказ,ч;

$T_в$ – среднее время восстановления, ч.

В таблице 21 представлены расчёты коэффициента готовности по компонентам СКУД.

Таблица 21 – Расчёт коэффициента готовности

Наименование оборудования	Время наработки на отказ, час (не менее)	Время восстановления, час	Коэффициент готовности, $К_г$
Коммутатор Elsys-MB-Net	20000	6	0,9997
Контроллер Elsys-MB-SM-2A-ТП	20000	6	0,9997
Считыватель Elsys-SW10-EN	60000	6	0,9999
Электромагнитный замок «ML-200M»	100000	6	0,9999
Турникет Elsys-ST-TS100	30000	6	0,9998
Извещатель магнитоконтактный «ИО 102-16/2»	500000	6	0,9999
Процессор АРМ	15000	6	0,9996
Монитор АРМ	50000	6	0,9999

Для расчёта коэффициента готовности СКУД в целом нужно знать значимости показателя надежности элемента для общего показателя надежности СКУД, поэтому на данном этапе исследования не представляется возможным рассчитать коэффициент готовности СКУД, который согласно ГОСТ Р 53704-2009 [44] составляет 0,93.

3.5 Выводы по главе 3

В главе 3 разработано техническое задание на проектирование СКУД. Был проведён сравнительный анализ предложений наиболее востребованных потребителями, по критериям стоимости и функциям компонентов СКУД, а также комплексная оценка по клиентоориентированности, на основе которых выбрано решение СКУД Elsys с ПО «Бастион» компании ООО «ЕС-пром». Подобрано оборудование для восьми точек доступа, а также источники бесперебойного питания, которые обеспечивают нормальную работу системы контроля и управления доступом при отключении централизованного электроснабжения. Рассчитаны показатели надёжности СКУД.

4 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

4.1 Расчёт стоимости разработки системы контроля и управления доступом

Произведем расчет стоимости разработки системы контроля и управления доступом в соответствии со «Справочником базовых цен на проектные работы для строительства «Системы противопожарной и охранной защиты», одобренным и рекомендованным для применения Госстроем России (далее – справочник) [45]. Стоимость проектирования системы контроля и управления доступом определяется на основании базовых цен. В базовых ценах методики учитываются расходы на оплату труда всех участников выполняемых работ, содержание административно-управленческого персонала, отчисления на государственное социальное и медицинское страхование, материальные затраты, амортизационные отчисления на полное восстановление основных производственных фондов и расходы по всем видам их ремонта, арендная плата, налоги и сборы, установленные в законодательном порядке (без учёта налога на добавленную стоимость), а также прибыль.

В соответствии со справочником базовая цена разработки проектной документации рассчитывается по формуле:

$$Ц = (С_п) \times К_i, \quad (2)$$

где Ц – цена разработки проектной документации, тыс. руб;

$С_п$ – цена проектной документации, определённая по таблицам справочника, тыс. руб.;

$К_i$ – безразмерный повышающий коэффициент, отражающий инфляционные процессы на момент определения цены.

Базовые цены принимаем в зависимости от величины натуральных показателей: площади, объёма помещений проектирования в соответствии с справочником базовых цен на проектные работы. Уровень цен, содержащихся в

справочнике, установлен по состоянию на 01.01.1995 г. Повышающий коэффициент, отражающий инфляционные процессы на момент определения цены взят из письма Минстроя России от 05.03.2020 г. № 7581-ДВ/09 «Об индексах изменения сметной стоимости строительства в I квартале 2020 г.» и составляет 33,58. В соответствии со справочником цена разработки проектной документации на установку системы контроля и управления доступом составляет 3567 руб. В случае проектирования точек входа с двусторонним доступом используется повышающий коэффициент 1,5. Приведём расчёты по формуле (2) в таблице 22.

Таблица 22 – Результаты расчётов стоимости проектных работ

Проектирование системы контроля и управления доступом	Стоимость проектных работ, руб. с учётом повышающего коэффициента	
	1995 г.	2020 г.
Точки входа с двусторонним доступом – имеются	5350	179653

Таким образом, стоимость проектных работ составляет 179653 руб.

4.2 Расчёт стоимости оборудования системы контроля и управления доступом

Расчёт стоимости оборудования системы контроля и управления доступом производится на основании цен поставщика за единицу оборудования. Смета на приборы и оборудование представлена в таблице 23.

Таблица 23 – Смета на приборы и оборудование

Наименование	Количество, шт	Стоимость единицы, руб	Итого, руб
Контроллер Elsys-MB-SM-2A-ТП	8	10350,00	82800,00
Считыватель Elsys-SW10-EH	10	3030,00	30300,00
Магнитоконтактный извещатель «ИО 102-16/2»	8	56,00	448,00
Кнопка открытия двери без фиксации	12	56,00	672,00

Продолжение таблицы 23

Замок электромагнитный «ML-200M»	8	3733,00	29864,00
Коммутатор Elsys-MB-Net	1	6632,00	6632,00
Сервер IBM	4	19300,00	77200,00
Видеомагнитофон «VideoNova A40-IP-16»	1	18260,00	18260,00
Турникет Elsys ST-TS100	1	86270,00	86270,00
Замок электромеханический	1	1569,00	1569,00
Монитор	4	12320,00	49280,00
		Итого	383295,00

Приведены основные затраты на оборудование и материалы, стоимость кабельных изделий и элементов крепежа не учитывалась. Следовательно, общая стоимость приборов и оборудования составила 383295,00 руб.

4.3 Расчёт пусконаладочных работ

Стоимость монтажа системы контроля и управления доступом была определена согласно сборников сметных нормативов Российской Федерации ФЕРм-2001 (часть 10 «Оборудование связи») и ФЕР 81-02-09-2001 «Сборник 9. Строительные металлические конструкции». Приведённые в сборнике цены соответствуют уровню 2001 г. Смета на пусконаладочные работы приведена в таблице 24.

Таблица 24 – Смета на пусконаладочные работы

Вид работы	Прямые затраты, руб.	Оплата труда рабочих, руб.	Затраты труда рабочих, чел.-ч	Количество	Стоимость, руб.
Установка контроллеров	3968,08	304,01	35,64	8 шт.	31744,64
Установка считывателей	94,80	65,6	7,69	10 шт.	948,00
Установка магнитоконтактных извещателей	42,36	28,23	3,31	8 шт.	338,88
Установка замков электромагнитных	204,97	77,03	9,03	8 шт.	1639,76
Установка кнопок открытия	45,75	34,02	3,11	12 шт.	549,00

Продолжение таблицы 24

Прокладка кабеля, на 100 м	1801,24	943,72	98,1	1600 м	28819,84
Установка турникета	1223,41	519,86	1,68	1 шт.	1223,41
Установка блока бесперебойного питания	159,96	18,08	0,84	1 шт.	159,96
				Итого	65423,22

Итоговая стоимость пусконаладочных работ составляет 65423,22 руб. Индекс изменения стоимости по отношению к 2001 г. составляет 4,91 [46]. Общая стоимость пусконаладочных работ с учётом индекса изменения стоимости составит 68635,50 руб.

4.4 Расчёт технического обслуживания системы контроля и управления доступом в период эксплуатации

Системы контроля и управления доступом содержат оборудование, которое нуждается в текущем и периодическом техническом обслуживании. Например, датчики-извещатели могут эффективно работать при соблюдении правил эксплуатации, но на них негативно влияет целый ряд факторов – пыль, водяные пары, газы и др. Не стоит исключать и потенциальную возможность намеренной порчи оборудования злоумышленниками. Чтобы устранить негативное воздействие на компоненты системы контроля и управления доступом, проводят техническое обслуживание: проверка внешнего состояния и функционирования компонентов, при необходимости – корректировка настроек, проверка работоспособности. В соответствии с рекомендациями по техническому обслуживанию, разработанными производителями систем контроля и управления доступом, ежедневно выполняются:

- осмотр целостности технических средств защиты;
- проверка состояния шлейфов, датчиков-извещателей и другого оборудования (отсутствие повреждений, грязи, следов коррозии и т.п.);
- определение работоспособности компонентов системы, целостность пломб опломбированных приборов.

Ежемесячно рекомендуется проверять:

- надёжность подключений к источнику питания, работоспособность резервного источника питания;

- тестирование на работоспособность компонентов системы контроля и управления доступом;

- замена неработоспособных, изношенных, дефектных компонентов.

Ежегодно выполняется полная проверка состояния всех компонентов системы контроля и управления доступом и проверка заземления системы в целом, а также каждого компонента в отдельности. Один раз в три года проверяют изоляцию токоведущих элементов на целостность. Расчет затрат на техническое обслуживание приводится в таблице 25.

Таблица 25 – Расчет стоимости обслуживания системы контроля и управления доступом

Наименование оборудования	Количест-во, шт.	Стоимость обслуживания единицы, руб.	Стоимость в месяц, руб.	Стоимость в год, руб.
Магнитоконтактный извещатель«ИО 102-16/2»	8	120,00	960,00	11520,00
Кнопка открытия двери без фиксации	12	–	1123,00	13476,00
Замок электромагнитный «ML-200 M»	8	130,00	1040,00	12480,00
Коммутатор Elsys-MB-Net	1	189,00	189,00	2268,00
Сервер IBM	4	132,00	528,00	6336,00
Видеомагнитофон «VideoNova A40-IP-16»	1	78,00	78,00	936,00
Турникет Elsys ST-TS100	1	169,00	169,00	2028,00
Замок электромеханический	1	-	-	-
Монитор	4	-	-	-
Контроллер Elsys-MB-SM-2A-ТП	8	109,00	872,00	10464,00
Считыватель Elsys-SW10-EH	10	99,00	990,00	11880,00
Итого				71388,00

В обязанности исполнителей, кроме работ по техническому обслуживанию системы контроля и управления доступом, входит ещё и ведение необходимой документации (журналов проверок). График проведения технического обслуживания оборудования СКУД на 2020 г. приводится в таблице 26.

Таблица 26 – График проведения технического обслуживания на 2020 г.

Наименование оборудования	Вид обслужи-вания	1 квартал			2 квартал			3 квартал			4 квартал		
		01	02	03	04	05	06	07	08	09	10	11	12
Магнитоконтактный извещатель	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					
Замок электромагнитный «ML-200 M»	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка		×		×			×			×		
	Профи-лактика							×					
Коммутатор Elsys-MB-Net	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					
Сервер IBM	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					
Видеомагнитофон «VideoNova A40-IP-16»	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					
Турникет Elsys ST-TS100	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					
Считыватель Elsys-SW10-EH	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка		×			×			×			×	
	Профи-лактика							×					
Контроллер Elsys-MB-SM-2A-ТП	Осмотр	×	×	×	×	×	×	×	×	×	×	×	×
	Проверка			×			×			×			×
	Профи-лактика							×					

В таблицу включены следующие виды технического обслуживания: внешний осмотр оборудования, проверка его работоспособности; профилактические работы. Нормативы по стоимости обслуживания в настоящей работе представлены ООО «Феорана», основным видом деятельности которого является монтаж, техническое обслуживание и ремонт средств обеспечения безопасности на промышленных объектах.

Расчет затрат по статье «Налоги, отчисления в бюджет и внебюджетные фонды» включает отчисления по установленным законодательством нормам в пенсионный фонд, в фонд социальной защиты населения, на обязательное медицинское страхование, на другие социальные нужды.

Затраты по данной статье выполняются по формуле

$$Сн = \frac{(Созп + Сдзп) \cdot (Сс.н.+ Сстр)/}{100}, \quad (3)$$

где $С_{озп}$ – основная зарплата работников банка, руб.;

$С_{дзп}$ – дополнительная зарплата работников банка, руб.;

$О_{с.н}$. – ставка социального налога (принять 30,2 %);

$О_{стр}$ – ставка страховых взносов по прочим видам обязательного страхования (принять 0,7%);

Сн = (22000 + 6300) · 30,2+0,7 · 100 = 8616,6руб.

4.5 Вывод по главе 4

В данном разделе произведены расчёты стоимости разработки системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга (179653,00 руб.), расчёты стоимости оборудования разработанной системы контроля и управления доступом – 383295,00 руб., расчёт затрат на пусконаладочные работы – 68635,50 руб., расчёт технического обслуживания системы контроля и управления доступом – 71388,00руб. Общие затраты на внедрение разработанной системы контроля и управления доступом филиала ПАО КБ «Восточный» в г. Юрга составляют 702971,50 руб.

5 Социальная ответственность

5.1 Описание рабочего места сотрудника охраны

Рабочее место сотрудника охраны расположено в вестибюле филиала банка ПАО КБ «Восточный» в г. Юрга. Размеры фойе: длина 7,0 м; ширина 4,0 м; высота 2,7 м. На рабочем месте сотрудника охраны работает один человек. Сотрудником охраны используется оборудование автоматизированного рабочего места (компьютер, многофункциональное устройство, телефон) и материалы (канцелярские товары), мебель (кресло компьютерное «Престиж»). Рабочее место сотрудника охраны соответствует эргономическим требованиям, приведённым в ГОСТ 12.2.032-78 [47]. Распорядок рабочего времени сотрудника охраны: восьмичасовой рабочий день, практически 100 % рабочего времени сотрудник находится внутри помещения. В помещении комбинированное освещение – естественное за счёт оконных проёмов и искусственное (люминесцентные лампы Philips 18 Вт G13 4000 K). Отопление водяное. Вентиляция осуществляется естественным путём через оконные проёмы. В помещении смонтирован кондиционер Electrolux EACS-07 HFE/N3.

В Приказе Министра труда и социальной защиты РФ № 601н «Об утверждении Правил по охране труда при осуществлении охраны (защиты) объектов и (или) имущества» от 15.11.2017 г. [48] официально признан факт наличия профессионального риска повреждения здоровья сотрудников охраны при осуществлении ими трудовых функций и приведен перечень отдельных вредных и (или) опасных производственных факторов: противоправные действия других лиц; последствия неправильного обращения с огнестрельным оружием и специальными средствами; пожар или взрыв; физические и нервно-психические перегрузки; движущиеся транспортные средства, грузоподъемные машины, перемещаемые материалы, подвижные части оборудования; повышенная или пониженная температура воздуха рабочей зоны; повышенный

уровень шума или вибрации; повышенная запыленность или загазованность воздуха; недостаточная освещенность рабочей зоны; повышенная или пониженная влажность и повышенная подвижность воздуха рабочей зоны; расположение рабочего места на высоте относительно поверхности земли (пола); замыкание электрических цепей через тело работника. Учитывая специфику рассматриваемого объекта, считаем, что можно пренебречь влиянием следующих факторов на сотрудника охраны банка: взрыв; движущиеся транспортные средства, грузоподъемные машины, перемещаемые материалы, подвижные части оборудования; повышенный уровень вибрации; повышенная запыленность или загазованность воздуха; расположение рабочего места на высоте относительно поверхности земли (пола).

5.2 Анализ выявленных вредных факторов

5.2.1 Шум

На рабочем месте сотрудника охраны основным источником шума является компьютер. Нормирование шума производится в соответствии с СН 2.2.4/2.1.8.562-96, нормативное значение эквивалентного уровня звука составляет 65 дБА [49]. Результаты измерений уровня шума на рабочем месте сотрудника охраны согласно данным, полученным от администрации банка, составили 60 дБА, что свидетельствует о допустимом уровне шума. Вследствие этого на анализируемом рабочем месте не используются средства защиты от шума.

5.2.2 Электромагнитное излучение

Нормирование воздействия электромагнитных полей на человека производится согласно СанПиН 2.2.4.1340-03 [50]. Таблица 26 показывает результаты измерений электромагнитных полей на рабочем месте сотрудника охраны согласно данным, полученным от администрации банка. Сравнение

результатов измерений с нормативными значениями позволяет прийти к выводу, что превышение нормативов отсутствует.

Таблица 26 – Результаты измерений электромагнитного поля

Показатель	Норматив	Факт	Класс условий труда
Напряженность электростатического поля, кВ/м	15	3,5	2
Напряженность переменного электрического поля, В/м			
Диапазон от 5 до 2 кГц	25	14	2
Диапазон от 2 до 400 кГц	2,5	0,35	2
Плотность магнитного потока, нТл			
Диапазон от 5 до 2 кГц	250	46	2
Диапазон от 2 до 400 кГц	25	2	2

На анализируемом рабочем месте не используются средства коллективной и индивидуальной защиты вследствие допустимого уровня воздействия электромагнитных полей.

5.2.3 Микроклимат

Нормирование параметров микроклимата производится в соответствии с СанПиН 2.2.4.3359-16 [51]. В таблице 27 приводятся результаты измерений температуры в помещении, относительной влажности и скорости движения воздуха в тёплое и холодное время года на рабочем месте сотрудника охраны согласно данным, полученным от администрации банка.

Таблица 27 – Результаты измерений параметров микроклимата

Показатель	Факт	Оптимальное значение	Допустимое значение	Класс условий труда
В помещении, категория I а, теплый период				2
Температура, °С	23	23–25	21–28	2
Скорость движения воздуха, м/с	0,04	Не более 0,1	Не более 0,2	1
Влажность воздуха, %	50	40–60	15–75	1
В помещении, категория I а, холодный период				2

Продолжение таблицы 27

Температура, °С	21	22–24	20–25	2
Скорость движения воздуха, м/с	0,04	не более 0,1	не более 0,1	1
Влажность воздуха, %	21	40–60	15–75	2

Анализируя данные таблицы 27, приходим к выводу об отсутствии превышения нормируемых показателей.

Для поддержания допустимых значений параметров микроклимата на анализируемом рабочем месте предусмотрено: водяное отопление, естественная вентиляция через оконные проёмы, в помещении имеется кондиционер.

5.2.4 Освещённость

5.2.4.1 Нормирование параметров освещённости

Результаты измерений освещенности на рабочем месте сотрудника охраны в комнате охраны согласно данным, полученным от администрации банка, приведены в таблице 28.

Таблица 28 – Результаты измерений освещённости

Показатель	Факт	Норматив	Класс условий труда
Коэффициент естественной освещённости КЕО, %	2,3	0,5	2
Общая освещенность, лк	600	300	2
Коэффициент пульсации, %	5,2	10	2

Параметры освещённости нормируются согласно СанПиН 2.2.1/2.1.1.1278-03 «Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий», СП 52.13330.2016 «Естественное и искусственное освещение» [52, 53]. Как

следует из анализа данных, приведённых в таблице 17, фактические значения параметров освещённости не превышают нормативные.

На рабочем месте сотрудника охраны контролируются параметры освещённости (один раз в год согласно приказу КБ «Восточный»), при необходимости заменяются неисправные осветительные приборы. Для уменьшения отражённой блёсткости на мониторе АРМ имеется антибликовый фильтр TY-AR50P12W.

5.2.4.2 Расчёт параметров освещённости

Расчёт параметров освещённости был проведён для помещения длиной 7,00 м, шириной 4,00 м, высотой 2,70 м с общей площадью 28,00 м^2. Потолок подвесной из поливинилхлоридных панелей белого цвета. Стены из гипсокартона светло-бежевого цвета. Пол – линолеум светло-коричневого цвета. Высота рабочего стола над полом равна 0,75 м. Освещённость должна соответствовать выполнению зрительной работы очень высокой точности (наименьший размер объекта различения 0,15–0,3 мм, разряд зрительной работы – 2, подразряд зрительной работы – Г, фон – светлый, контраст объекта с фоном – большой).

Для данного помещения предлагаем систему общего равномерного освещения, в качестве источника света – светодиодный модуль Varton 2835 SMD 18×0.5W LED = 9W со световым потоком 4200 лм.

Световой поток Ф (лм) рассчитываем по формуле:

$$\Phi = (E \cdot k \cdot S \cdot Z)/(n \cdot \eta), \quad (4)$$

где E – минимальная освещённость, лк;

k – коэффициент запаса;

S – площадь комнаты охраны, м^2;

Z – коэффициент неравномерности освещения;

n – число ламп в комнате охраны;

η – коэффициент использования светового потока.

Согласно СанПиН 2.2.2/2.4.1340-03 [50] минимальная освещённость равна 300 лк; значение коэффициента запаса для светодиодных светильников составляет 1,1; значение коэффициента неравномерности освещения принимается равным 1,0 [60].

Индекс помещения i определяем по формуле:

$$i = S/(h\cdot(A+B)), \quad (5)$$

где h – высота подвеса светильников над рабочей поверхностью, м;

A – длина помещения, м;

B – ширина комнаты охраны, м.

Рассчитаем высоту подвеса светильников над рабочей поверхностью:

$$h = h_{min} - h_{рп}, \quad (6)$$

где h_{min} – минимально допустимая высота подвеса светильников над поверхностью пола, м;

$h_{рп}$ – высота рабочей поверхности над полом, м.

h = 2,90 – 0,75 = 2,15 м.

i = 28/(2,15·(7+4)) = 1,18 м ≈ 1,2 м.

Определяем наивыгоднейшее соотношение λ для расположения светильников и рассчитаем расстояние между светильниками L (м):

$$L = \lambda\cdot h, \quad (7)$$

L = 1,3·2,15 ≈ 2,8 м.

Рассчитаем расстояние от стены комнаты охраны до крайнего ряда светильников l (м):

$$l = \lambda/h, \quad (8)$$

l = 2,8:3 = 0,93 м.

Учитывая размеры комнаты охраны, размеры светодиодной панели (595×595×100 мм), расстояния между светильниками, приходим к выводу, что число светильников в ряду должно быть три, число рядов – один. Значение

коэффициента отражения потолка $\rho_п$ равно 70 % и коэффициента отражения стен $\rho_с$ равно 30 %. Следовательно, при этих условиях коэффициент использования светового потока составит 0,44. Подставим полученные данные в формулу для определения светового потока одного светильника.

Ф = (300·1,1·28·1)/(3·0,44) = 7000 лм.

Сравнивая расчётное значение со световым потоком предлагаемого источника света, приходим к выводу, что для обеспечения необходимой освещённости следует добавить дополнительно ряд светодиодных панелей. В этом случае рассчитаем величину светового потока.

Ф = (300·1,1·28·1)/(6·0,44) = 3500 лм.

Система общего освещения комнаты охраны состоит из шести светильников, расположенных в два ряда по три модуля, по схеме, представленной на рисунке 25.

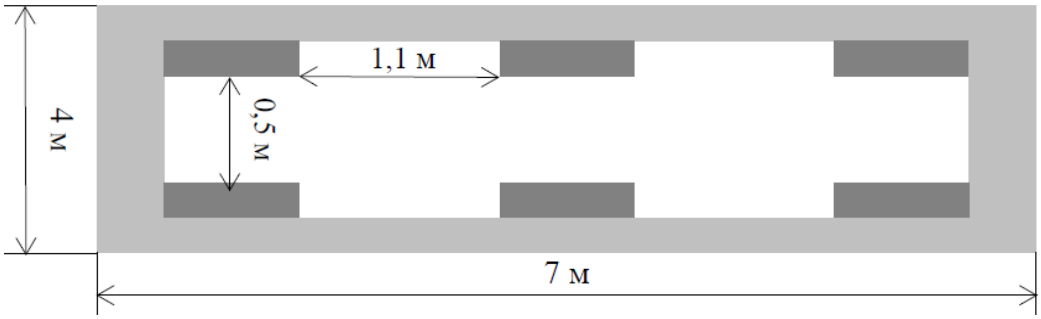


Рисунок 25 – Схема расположения светодиодных модулей

5.3 Анализ выявленных опасных факторов

5.3.1 Электробезопасность

На рабочем месте сотрудника охраны возможно получение травмы вследствие воздействия электрического тока. При поражении работника электрическим током возможна остановка сердца, прекращение дыхания из-за паралича мышц груди, шок. Продолжительное нахождение в состоянии шока может привести к летальному исходу.

Согласно Р 12.1.019-2009 безопасность работников от поражения электрическим током обеспечивается организационно-техническими мероприятиями, конструктивными особенностями приборов, техническими способами и средствами защиты [54].

Напряжение электросетей 380/220 В. Их эксплуатация, а также контроль за техническим состоянием осуществляется в соответствии с требованиями нормативных документов по электроэнергетике специализированной организацией, имеющей на данный вид деятельности соответствующую лицензию. Для предотвращения травматизма по причине воздействия электрического тока на рассматриваемом объекте проводятся своевременное профилактическое обслуживание (один раз в месяц согласно утверждённому плану) и ремонт действующих электроприборов (по необходимости). С целью защиты от поражения электрическим током на рабочем месте сотрудника охраны используемое электрооборудование заземлено согласно ПУЭ [24]. В помещениях банка использовано непроводящее половое покрытие.

5.3.2 Пожарная безопасность

Возгорание на рассматриваемом объекте может возникнуть вследствие нарушения правил техники безопасности, целостности электрической проводки, поломки электроприборов. С целью уменьшения риска возникновения пожара на объекте разработан ряд мероприятий. К организационным мероприятиям относятся: проведение инструктажей, обучение пожарно-техническому минимуму, издание приказов по вопросам усиления пожарной безопасности. К эксплуатационным мероприятиям относятся правильная эксплуатация электрооборудования, профилактические ремонты, осмотры и испытания оборудования и устройств, в том числе систем безопасности. К техническим мероприятиям относятся: соблюдение противопожарных норм и правил при устройстве и установке систем безопасности, кондиционирования, подвода электропроводки, защитного

заземления. К режимным мероприятиям относится запрещение курения в неустановленных местах.

Для уменьшения риска возникновения пожара по причине нарушения целостности электропроводки в помещениях филиала банка состояние электропроводки проверяется один раз в полгода согласно ведомственному приказу в соответствии с установленным графиком. Электропроводка выполнена кабелем с оболочкой из материала, не распространяющего горение.

В целях обеспечения пожарной безопасности на посту охраны имеется инструкция о порядке действий на случай возникновения пожара в дневное и ночное время, телефон, электрический фонарь, средство индивидуальной защиты органов дыхания и зрения человека от токсичных продуктов горения (газодымозащитный противогаз «Шанс» с временем защиты от продуктов горения не менее 60 мин).

В помещении офиса банка имеется один эвакуационный выход. Пути эвакуации не загромождены. Высота эвакуационного выхода составляет 2,3 м; ширина 0,96 м согласно требованиям СП 1.13130.2009 «Системы противопожарной защиты. Эвакуационные пути и выходы» [55].

Помещение оборудовано системой автоматической пожарной сигнализации на базе приемно-контрольного прибора «Сигнал–20П» с использованием дымовых пожарных извещателей. Для оповещения персонала о пожаре во всех помещениях (с постоянным или временным присутствием людей) установлены светозвуковые оповещатели «Свирель-2». Принятые решения соответствуют требованиям НПБ 110–03 [27], НПБ 104–03 [28]. Расчётное время прибытия подразделения пожарной охраны при средней скорости движения 40 км/ч составляет менее 5 мин, что соответствует требованиям Федерального закона от 22.07.2008 N 123-ФЗ (ред. от 27.12.2018) «Технический регламент о требованиях пожарной безопасности» [56].

Анализируемый объект оснащён первичными средствами пожаротушения в соответствии с нормами, установленными НПБ 166-97 «Пожарная техника. Огнетушители. Требования к эксплуатации» [57]. Учитывая пожарную

нагрузку, в помещении возможны классы пожара А (горение твёрдых веществ, сопровождающееся тлением) и Е (горение электрооборудования, находящегося под напряжением). Руководствуясь требованиями Правил противопожарного режима в Российской Федерации, в помещении установлено три порошковых огнетушителя марки ОП-3(з) (производитель – ООО «Ярпожинвест», г. Ярославль). Огнетушители промаркированы, на них заведены паспорта, заведен журнал учета наличия, проверки и состояния первичных средств пожаротушения.

5.3.3 Противоправные действия других лиц и последствия неправильного обращения с огнестрельным оружием и специальными средствами

При выполнении задач профессиональной деятельности у сотрудника охраны имеется угроза жизни и здоровью в результате возможных противоправных действий других лиц (например, вооруженное нападение, захват заложников). При возникновении противоправной ситуации – нападении на объект или угрозе возникновения террористической угрозы – сотрудник охраны должен немедленно воспользоваться кнопкой экстренного вызова полиции, а также по средствам связи доложить группе быстрого реагирования, а также принять меры к задержанию правонарушителей. При этом его действия регламентируются Законом РФ от 11 марта 1992 г. N 2487-1 «О частной детективной и охранной деятельности в Российской Федерации», сотрудник охраны банка имеет право применять физическую силу, из спецсредств разрешено использование резиновых палок. Применение охранником физической силы, специальных средств или огнестрельного оружия с превышением своих полномочий, крайней необходимости или необходимой обороны влечет за собой ответственность, установленную законом. Для уменьшения возможного ущерба жизни и здоровью сотрудника охраны Правилами по охране труда при осуществлении охраны (защиты) объектов и (или) имущества устанавливается, что заступить на охрану объекта может лишь

лицо не моложе восемнадцати лет и подтвердившее свою квалификацию прохождением обучения. Также Правила упоминают об обязательности применения соответствующих трудовому законодательству РФ режимов труда и отдыха и о необходимости обеспечения сотрудников спецодеждой. Работник, не прошедший инструктаж по мерам безопасности при осуществлении охраны объекта, в т.**ч.** при обращении с огнестрельным оружием и спецсредствами, если охрана объекта предусматривает ношение и применение оружия и спецсредств, не вправе приступить к выполнению своей трудовой функции. При осуществлении охраны объектов запрещены: выполнение работ, не предусмотренных трудовыми обязанностями или договорными обязательствами; уход с поста, за исключением случаев оказания помощи пострадавшим при аварийных ситуациях, предотвращения правонарушений и задержания правонарушителей; самостоятельное устранение недостатков в электроснабжении и неисправностей технических средств охраны. Во избежание ущерба жизни и здоровью, сотрудник охраны не должен предпринимать действий, которые могут стимулировать агрессию нападающих и причинение вреда людям, находящимся в помещении банка.

5.4 Охрана окружающей среды

На рабочем месте сотрудника охраны образуется небольшое количество твёрдых бытовых отходов разных видов – пищевые, пластик, бумага, текстиль и др. Отходы принадлежат к IV–V классам опасности согласно Федеральному закону «Об отходах производства и потребления» от 24.06.1998 № 89-ФЗ. Отходы накапливаются в контейнере и вывозятся на спецмашинах для захоронения на полигоне твёрдых бытовых отходов согласно договору.Офис банка присоединён к централизованной системе канализации, куда сливаются образующиеся жидкие бытовые отходы.

5.5 Защита в чрезвычайных ситуациях

К потенциальным чрезвычайным ситуациям (ЧС) природного характера, возможным в г. Юрга, относятся: землетрясения, ураганы, наводнения. ГУ МЧС России по Кемеровской области–Кузбассу своевременно информирует объекты о ЧС. На анализируемом объекте разработан план мероприятий по обеспечению безопасности сотрудников в условиях ЧС.

Кроме того, на рассматриваемом объекте могут возникнуть ЧС техногенного характера (внезапное обрушение здания, аварии на коммунальных системах снабжения).

С целью защиты работников и территории от ЧС природного и техногенного характера, опасностей, возникающих при ведении военных действий или вследствие этих действий предприятие создаёт и содержит в постоянной готовности необходимые защитные сооружения и организации гражданской обороны в соответствии с федеральными законами РФ от 21.12.94 №66 «О защите населения и территорий от чрезвычайных ситуаций техногенного характера», от 12.02.98 №28 «О гражданской обороне» и постановлением правительства РФ №620 от 10.06.99 «О гражданских организациях гражданской обороны».

Т.к. анализируемый объект находится на первом этаже жилого здания на арендуемых площадях, меры по предотвращению обрушения здания реализует арендодатель: создана специальная комиссия, которая с периодичностью раз в полгода проводит осмотр здания и выносит предписания по необходимым мерам, а также следит за их выполнением.

5.6 Выводы по главе 5 «Социальная ответственность»

Результаты проведённого анализа вредных и опасных производственных факторов свидетельствуют, что они соответствуют нормативам.

Для обеспечения безопасной жизнедеятельности на объекте приняты следующие меры:

а) уровень шума на рабочем месте сотрудника охраны – 60 дБА (допустимый), средства защиты не требуются;

б) параметры электромагнитного поля допустимые, средства защиты не требуются;

в) параметры микроклимата не превышают нормируемых показателей. Для поддержания допустимых значений предусмотрено: водяное отопление, естественная вентиляция, кондиционер;

г) фактические значения параметров освещённости не превышают нормативные, предложена модернизация системы освещения за счет использования более экономичных светодиодных светильников Varton 2835 SMD 18×0.5W LED = 9W;

д) для предотвращения опасности поражения электрическим током применяется защитное заземление и непроводящее половое покрытие;

е) на объекте установлена автоматическая пожарная сигнализация, объект обеспечен первичными средствами пожаротушения согласно нормам;

ж) деятельность сотрудника охраны характеризуется наличием угрозы жизни и здоровью в результате возможных противоправных действий других лиц;

з) анализируемый объект не оказывает значительного вредного воздействия на окружающую среду.

Заключение (выводы)

Выпускная квалификационная работа содержит в своей основе материалы производственной и преддипломной практик, анализ нормативно-технической документации, научной литературы по проблеме исследования. При выполнении выпускной квалификационной работы в результате анализа нормативных документов, технической и специальной литературы были решены поставленные задачи. Изучен зарубежный и отечественный опыт в сфере применения систем контроля и управления доступом банковских объектов, рассмотрены современные тенденции в их использовании. К ним относятся:

- использование многофункциональных СКУД (контроль доступа, учёт рабочего времени персонала и др.);

- биометрическая идентификация;

- доступ по смартфону;

- в связи с неблагополучной ситуацией по коронавирусной инфекции интеграция СКУД с пирометрами или тепловизорами для автоматизации процесса выявления лиц с повышенной температурой с последующим недопуском их на рабочее место и направлением на консультацию к врачу.

Дана характеристика исследуемого объекта – филиала банка ПАО КБ «Восточный» в г. Юрга, рассмотрена применяемая в настоящее время система обеспечения безопасности его функционирования.

Отмечено, что используемая в настоящее время система контроля и управления доступом нуждается в модернизации, которая была осуществлена проектным решением: разработано техническое задание, на основе которого подобрано оборудование для восьми точек доступа,

Предварительное обследование объекта защиты, анализ применяющихся систем безопасности позволили разработать техническое задание на проектирование СКУД. Был проведён сравнительный анализ предложений,

четырёх российских и зарубежных производителей, отмеченных в качестве наиболее востребованных потребителями, по критериям стоимости и функциям компонентов СКУД, а также комплексная оценка по клиентоориентированности, на основе которых выбрано решение СКУД Elsys с ПО «Бастион» компании ООО «ЕС-пром» (г. Самара). Подобрано оборудование для восьми точек доступа, а также источники бесперебойного питания, которые обеспечивают нормальную работу системы контроля и управления доступом при отключении централизованного электроснабжения. Рассчитаны показатели надёжности СКУД.

Технические решения, принятые при разработке СКУД филиала банка ПАО КБ «Восточный» в г. Юрга, соответствуют требованиям санитарно-гигиенических, противопожарных и других нормативов, действующих на территории Российской Федерации, и обеспечивают безопасное для жизни и здоровья работников и клиентов функционирование объекта при соблюдении предлагаемых мероприятий.

В работе произведён расчёт экономических затрат на внедрение СКУД филиала банка ПАО КБ «Восточный» в г. Юрга, включающий стоимость проектирования, оборудования и материалов, установки, пусконаладочных работ. Общие затраты составили 702971,50руб. Для обеспечения надёжной эксплуатации СКУД разработан график её проверки и технического обслуживания на 2019 г.

В выпускной квалификационной работе проведена оценка воздействия вредных и опасных производственных факторов на рабочем месте сотрудника охраны, а также ущерба, наносимого функционированием филиала банка ПАО КБ «Восточный» в г. Юрга, окружающей среде.

Список использованных источников

1. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М.: Стандартинформ, 2009. – 63 с.

2. Пресс-релизы [Электронный ресурс] / ГУ МВД РФ по г. Москва. – Режим доступа: https://77.мвд.рф/folder/6000313. Дата обращения: 15.05.2020 г.

3. Новости [Электронный ресурс] / Российская газета. – Режим доступа: https://rg.ru/news.html. Дата обращения: 19.05.2020 г.

4. Проектирование СКУД: эксперты советуют [Электронный ресурс] / Системы безопасности. – Режим доступа: lib.secuteck.ru/articles2/sys_ogr_dost/proektirovanie-skyd-eksperti-sovetyut. Дата обращения: 25.05.2020 г.

5. Мобильная идентификация в СКУД - смартфон вместо пропуска [Электронный ресурс] / Системы контроля. Управление доступом. – Режим доступа: https://www.drdoors-msc.ru/. Дата обращения: 20.05.2020 г.

6. Р 78.36.005-2011 Выбор и применение систем контроля и управления доступом [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/1200071688. Дата обращения: 16.04.2020 г.

7. Шакер И.Е. Использование биометрической аутентификации и перспективы ее применения в банковской системе России // Экономика. Налоги. Право. – 2016. – №5. – С. 18–26.

8. М.Н. Симаков. СКУД в банке: выбираем оптимальное решение / СКУД. Антитеррроризм. – М.: «ДМК Пресс», 2017. – 209 с.

9. Евдокимов Н.О. Система контроля и управления доступом по аудиоданным пользователя [Электронный ресурс] // Гаудеамус. – 2014. – №2 (24). – Режим доступа: https://cyberleninka.ru/article/n/sistema-kontrolya-i-upravleniya-dostupom-po-audiodannym-polzovatelya. Дата обращения: 06.05.2020.

10. Официальный интернет-сайт компании «PERCo» [Электронный

ресурс]. – Режим доступа: https://www.perco.ru. Дата обращения: 25.04.2020 г.

11. Международный форум «Технологии безопасности» [Электронный ресурс]. – Режим доступа: https://www.tbforum.ru/. Дата обращения: 26.04.2020 г.

12. Обзор решений СКУД [Электронный ресурс] / СКУД: обзоры и срезы рынка безопасности. – Режим доступа: http://www.techportal.ru/review/#obzory-resheniy-skud. Дата обращения: 22.04.2020 г.

13. Особенности СКУД: выбор экспертов [Электронный ресурс] / Системы безопасности. – Режим доступа: https://www.secuteck.ru/blog/tag/. Дата обращения: 25.05.2020 г.

14. Шипелов Д.А. Мобильный доступ, или смартфон вместо карты: сравнение решений, доступных на российском рынке // Системы безопасности. – 2019. – № 8. – С.45–49.

15. Бронников А.А. Сейсмическая система охраны объекта // Вестник КемГУ. Технические науки. – 2019. – №2-2. – с. 43– 56.

16. Борисов С.П. Единый специализированный объектовый протокол - повышение информативности для централизованной охраны // Алгоритм безопасности. – 2017. – № 4. – С. 23–39.

17. Байтимиров А.Д. Беспроводные технологии в промышленности [Электронный ресурс] // Вестник Казанского технологического университета. – 2014. – №14. – Режим доступа: https://cyberleninka.ru/article/n/besprovodnye-tehnologii-v-promyshlennosti. Дата обращения: 06.05.2020 г.

18. Терентьев А.М. Ложные срабатывания систем охраны [Электронный ресурс] // Национальные интересы: приоритеты и безопасность. – 2013. – №4. – Режим доступа: https://cyberleninka.ru/article/n/lozhnye-srabatyvaniya-antivirusnyh-sredstv . Дата обращения: 06.05.2020 г.

19. Р 78.36.032-2014. Инженерно-техническая укрепленность. Технические системы охраны. Требования и нормативы проектирования по защите объектов от преступных посягательств. – М.: НИЦ «Охрана», 2014. – 48 с.

20. РД 78.145-93 Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ. – М.: НИЦ «Охрана», 1993. – 52 с.

21. РД 78.147-93 Единые требования по технической укреплённости и оборудованию сигнализацией объектов. – М.: НИЦ «Охрана», 1993. – 31 с.

22. РД 78.148-94 Защитное остекление. Классификация, методы испытаний, применение. – М.: НИЦ «Охрана», 1994. – 66 с.

23. ГОСТ Р 50862-96 Системы безопасности. Инженерные средства защиты. Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/901704938. Дата обращения: 16.04.2020 г.

24. Правила устройства электроустановок. – 7-е изд. – М.: Изд-во НЦ ЭНАС, 2005. – 706 с.

25. Постановление Правительства Российской Федерации от 25.04.2012 г. N 390 «О противопожарном режиме» [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/902344800. Дата обращения: 19.04.2020 г.

26. СНиП 21-01-97* Пожарная безопасность зданий и сооружений [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/871001022. Дата обращения: 19.04.2020 г.

27. Приказ МЧС РФ от 18.06.2003 г. N 315 «Об утверждении норм пожарной безопасности «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией» (НПБ 110-03)» [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/901866575. Дата обращения: 19.04.2020 г.

28. Приказ МЧС РФ от 20.06.2003 г. N 323 «Об утверждении норм пожарной безопасности «Проектирование систем оповещения людей о пожаре в зданиях и сооружениях» (НПБ 104-03)» [Электронный ресурс] / Консорциум

КОДЕКС. – Режим доступа: http://docs.cntd.ru/document /901866573. Дата обращения: 19.04.2020 г.

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

30. Выбор системы контроля и управления доступом (СКУД) [Электронный ресурс] / ИНТЕМС. – Режим доступа: https://securityrussia.com/blog/vibrat_skud.html. Дата обращения: 21.04.2020 г.

31. Официальный интернет-сайт компании «Hikvision» [Электронный ресурс]. Режим доступа: https://hikvision.ru/. Дата обращения: 24.04.2020 г.

32. Постановление Правительства Российской Федерации от 16.02.2008 г. N 87 «О составе разделов проектной документации и требованиях к их содержанию» [Электронный ресурс] / Система ГАРАНТ. – Режим доступа: http://base.garant.ru/12158997/#ixzz6OYZWTIiO. Дата обращения: 22.04.2020 г.

33. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document /1200091365. Дата обращения: 16.04.2020 г.

34. СТО НОСТРОЙ 2.15.10-2011 Инженерные сети зданий и сооружений внутренние. Системы охранно-пожарной сигнализации, системы оповещения и управления эвакуацией, системы контроля и управления доступом, системы охранные телевизионные. Монтажные, пусконаладочные работы и сдача в эксплуатацию [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document /1200090184. Дата обращения: 20.04.2020 г.

35. ГОСТ 12.1.004-91 Система стандартов безопасности труда. Пожарная безопасность. Общие требования [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/9051953. Дата обращения:15.04.2020 г.

36. СанПиН 2.2.2/2.4.1340–03. Санитарно-эпидемиологические правила и нормативы «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [Электронный ресурс] /

Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/901865498. Дата обращения:22.04.2020 г.

37. ГОСТ 14254-2015 Степени защиты, обеспечиваемые оболочками (коды IP) [Электронный ресурс] / Консорциум КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/1200136066. Дата обращения:25.04.2020 г.

38. Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 N 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс] / ГАРАНТ. – Режим доступа: http://base.garant.ru/71629276/#ixzz6OYeSrd8q. Дата обращения:26.04.2020 г.

39. РД 30.03.1992 Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: НИЦ «Охрана», 1992. – 65 с.

40. Федеральные единичные расценки ФЕР-2020 / [Электронный ресурс] / Официальный сайт Минстроя России – Режим доступа: https://www.minstroyrf.ru/trades/view.fer-2020.php. Дата обращения:39004.2020 г.

41. ГОСТ 27.002-2015 Надежность в технике (ССНТ). Термины и определения [Электронный ресурс] / КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/1200136419. Дата обращения: 15.03.2020 г.

42. Луговцова Н.Ю. Расчеты надежности технических систем и техногенного риска: учебное пособие / Н.Ю. Луговцова; Юргинский технологический институт. – Томск: Изд-во Томского политехнического университета, 2019. – 342 с.

43. Малафеев С.И., Копейкин А.И. Надежность технических систем. Примеры и задачи: Учебное пособие. – СПб.: Издательство «Лань», 2012. – 320 с.

44. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования [Электронный ресурс] / КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/1200080466. Дата обращения: 15.03.2020 г.

45. Справочник базовых цен на проектные работы. М.: Минстрой РФ, 2020. – 156 с.

46. Справочники и нормативы [Электронный ресурс] / e-СМЕТА.ру. Сметный портал. – Режим доступа: http://www.e-smeta.ru/documents/idx/minregion/. Дата обращения: 20.03.2020 г.

47. ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования [Электронный ресурс] / КОДЕКС. – Режим доступа: http://docs.cntd.ru/document/1200003913 . Дата обращения:24.04.2020 г.

48. Приказ Министерства труда и социальной защиты РФ от 28 июля 2017 г. № 601н «Об утверждении Правил по охране труда при осуществлении охраны (защиты) объектов и (или) имущества» [Электронный ресурс] / ГАРАНТ. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71658592/. Дата обращения:24.05.2020 г.

49. СН 2.2.4/2.1.8.562–96. Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории застройки. Санитарные нормы [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/901703278. Дата обращения: 30.05.2019 г.

50. СанПиН 2.2.4.3359–16. Санитарно-эпидемиологичемские требования к физическим факторам на рабочих местах [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/420362948/. Дата обращения: 25.05.2019 г.

51. СанПиН 2.2.1/2.1.1.1278–03. Гигиенические требования к естественному, искусственному и совмещённому освещению жилых и общественных зданий [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/420362948/. Дата обращения: 25.05.2019 г.

52. ГОСТ 12.0.003-2015 ССБТ. Опасные и вредные производственные факторы. Классификация [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/4203634512/. Дата обращения: 25.05.2019 г.

53. СП 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95 [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/4206489/. Дата обращения: 30.05.2019 г.

54. ГОСТ Р 12.1.019-2009 Электробезопасность. Общие требования и номенклатура видов защиты [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/567290/. Дата обращения: 30.05.2019 г.

55. СП 1.13330.2009 Системы противопожарной защиты. Эвакуационные пути и выходы [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.ctd.ru /document/5285097215/. Дата обращения: 21.05.2019 г.

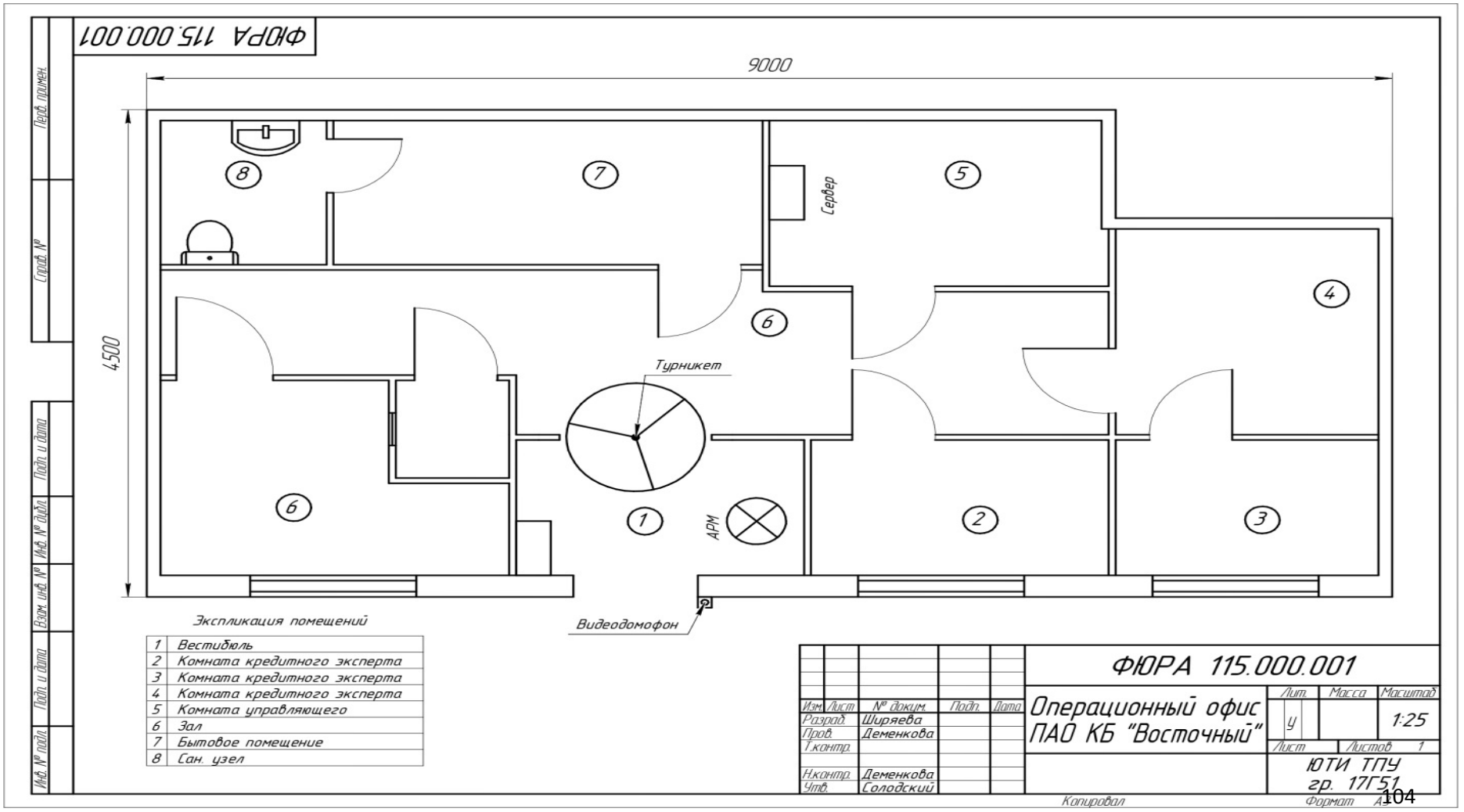
56. Технический регламент о требованиях пожарной безопасности: Федеральный закон от 22.07.2008 г. № 123-ФЗ (ред. от 27.12.2018) // Российская газета. – 2019. – № 2.

57. НПБ 166-97 Пожарная техника. Огнетушители. Требования к эксплуатации [Электронный ресурс] / Консорциум «Кодекс». – Режим доступа: http://docs.cntd.ru /document/4623591870/. Дата обращения: 21.05.2019 г.

Приложение А

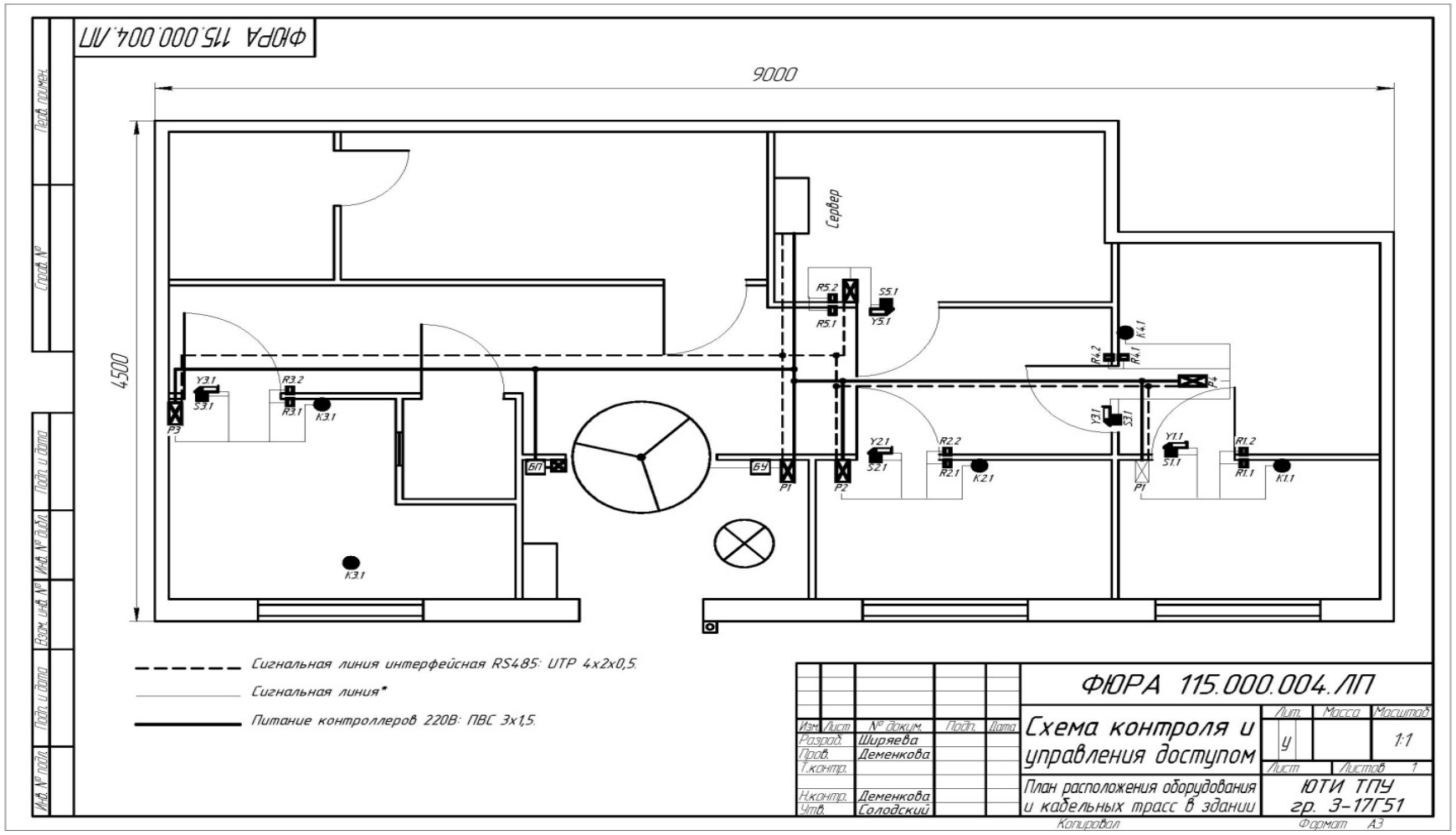
(обязательное)

Схема помещения офиса ПАО КБ «Восточный»



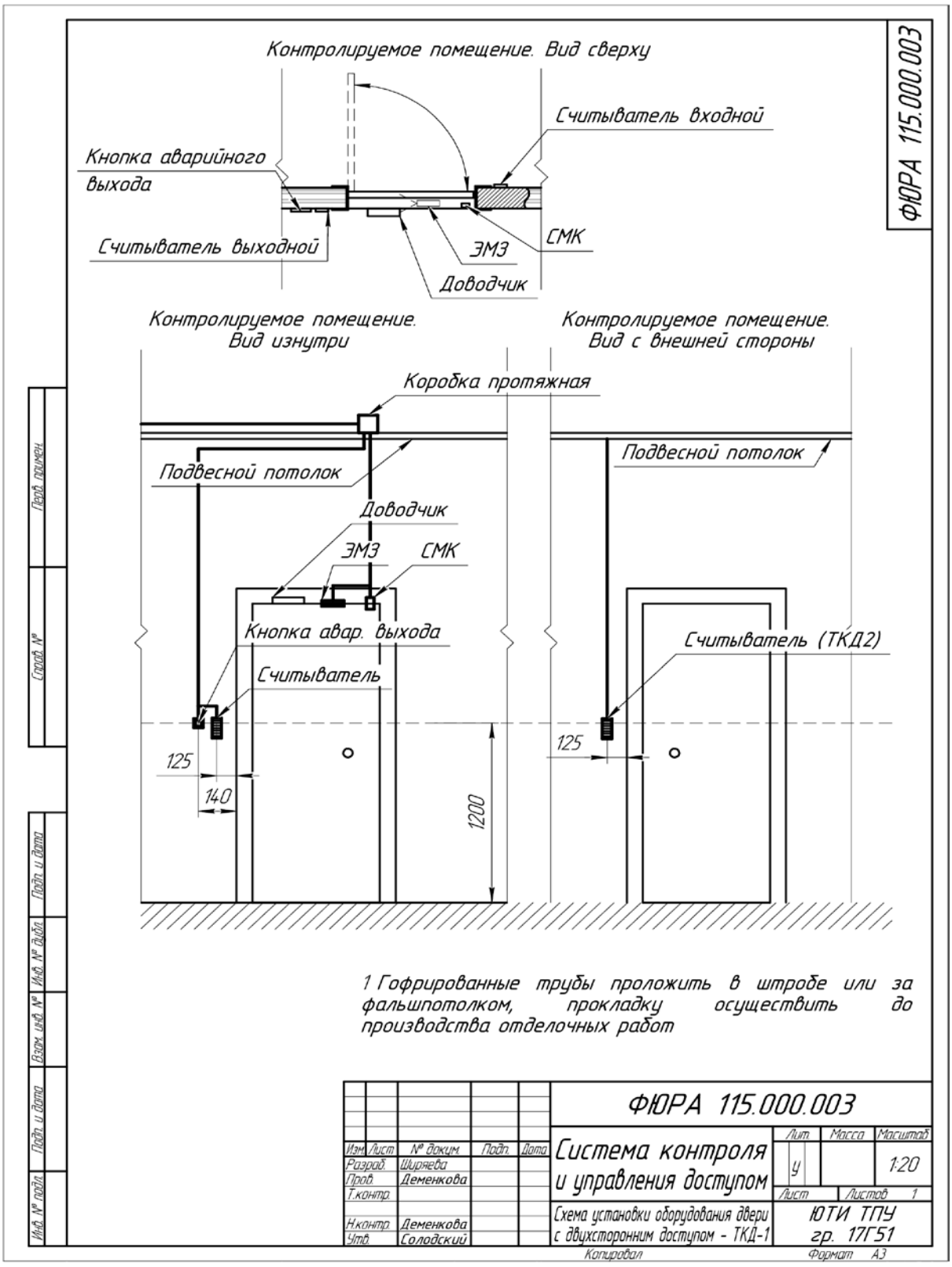
104

Приложение Б
(обязательное)
План расположения оборудования и кабельных трасс



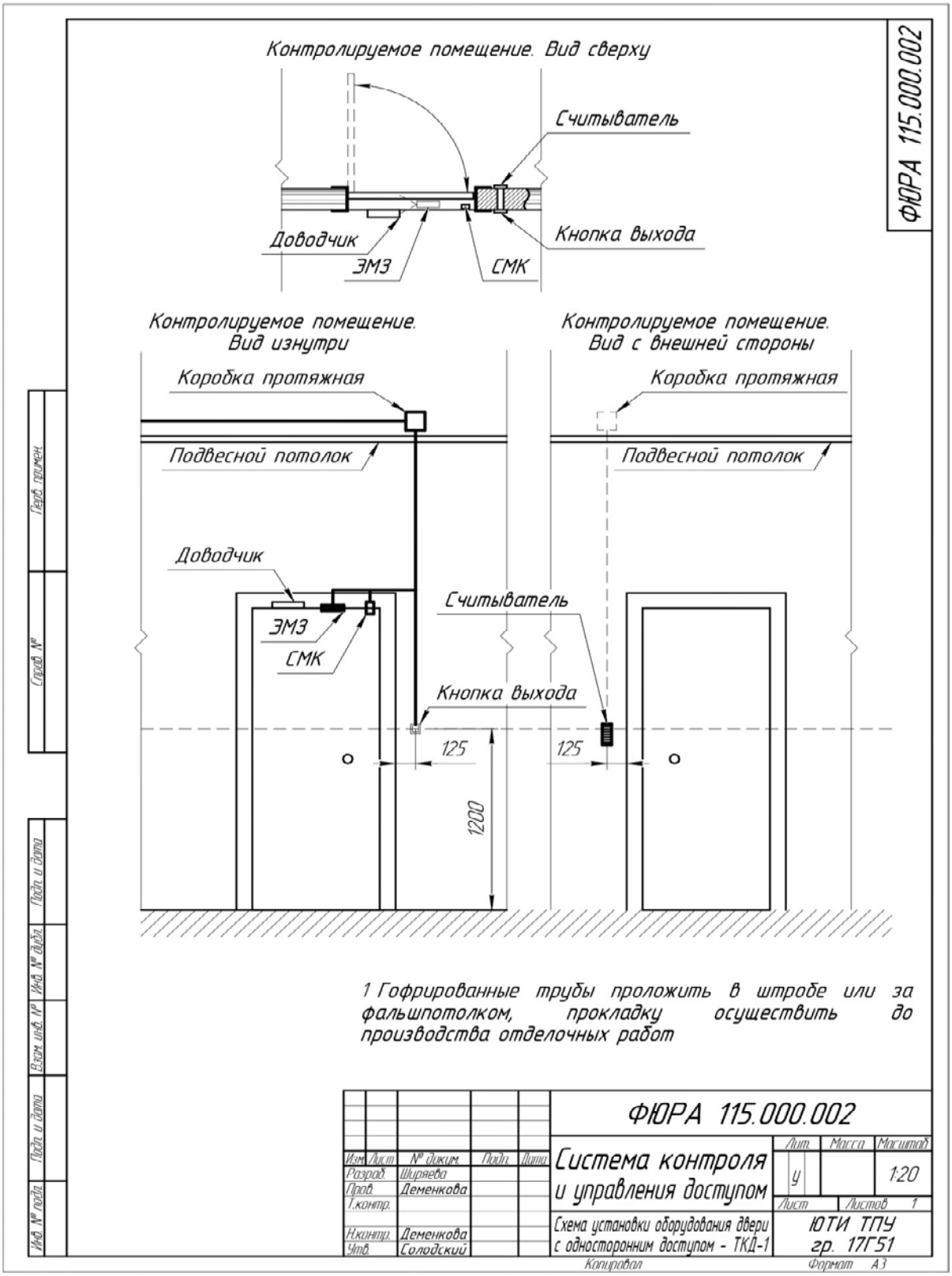
105

Приложение В
(обязательное)
Схема установки оборудования двери с двусторонним доступом



Приложение Г
(обязательное)

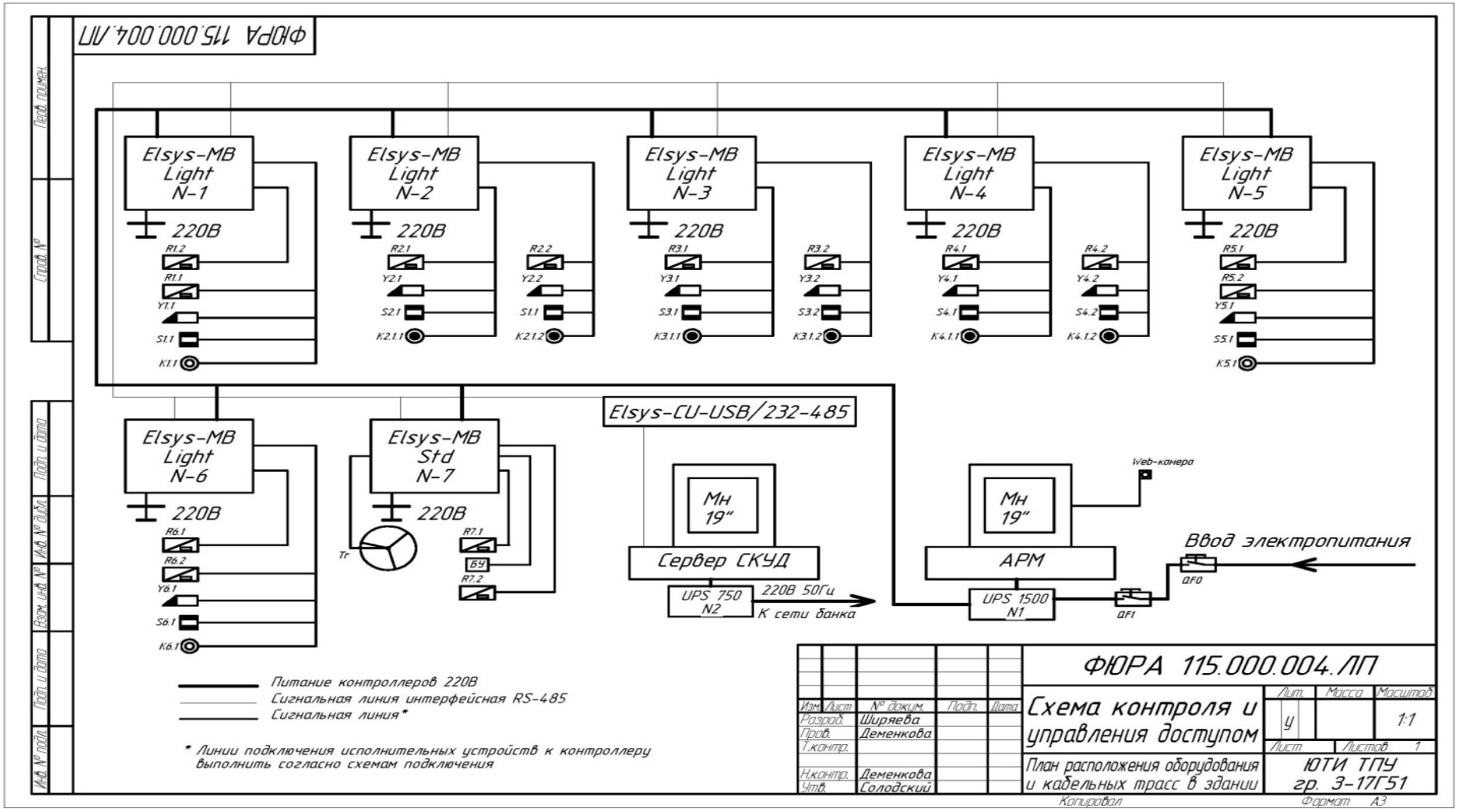
Схема установки оборудования двери с односторонним доступом



Приложение Д

(обязательное)

Структурная схема системы контроля и управления доступом



108