ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРА ПРИКЛАДНОЙ ИНФОРМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

СОВЕРШЕНСТВОВАНИЕ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОХРАНЫ В БЕЛГОРОДСКОМ ОТДЕЛЕНИИ ПЕНСИОННОГО ФОНДА РОССИИ

Выпускная квалификационная работа
обучающегося по направлению подготовки 38.03.05 «Бизнес-информатика»
очной формы обучения, группы 07001422
Тутова Ивана Михайловича

Научный руководитель:
старший преподаватель
Скрипина И.И.

БЕЛГОРОД 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Управление любым предприятием практически невозможно без использования компьютера. Компьютеры уже очень давно используются для ведения бухгалтерского и управленческого учета, управления складскими помещениями, закупками и ассортиментом. Однако современный бизнес требует более широкого применения информационных технологий в управлении предприятием.

В современной России активно развивается предпринимательская деятельность. Результатом этого является возникновение множества частных организаций. Среди множества других задач и проблем, у собственника бизнеса возникает необходимость обеспечить комфортные и безопасные условия труда для всех сотрудников организации.

Охраной труда называют разработку и применение мер, направленных на защиту здоровья и жизни человека в процессе труда, составляющих содержание человеческой деятельности. Это важнейшая составляющая безопасности жизнедеятельности человека.

Основными элементами работы организации в сфере безопасности являются повышение квалификации сотрудников, регулярные проверки, расследование и анализ чрезвычайных ситуаций, контроль за производством, состояние средств коллективной и индивидуальной защиты, политика найма и расстановки кадров. Сюда же можно отнести внедрение на предприятии комплексных информационных систем и программного обеспечения, которые позволят объединить все существующие системы безопасности в единый комплекс, а также автоматизировать контроль за безопасностью на объекте.

При значительных объемах управленческой информации, имеющихся на любом предприятии, контроль безопасности можно автоматизировать, использовав преимущества современных информационных технологий,

основанных на применении компьютеров и телекоммуникационных средств. Вследствие этого, на предприятиях массово внедряются автоматизированные информационные системы, позволяющие эффективно и точно управлять такой информацией.

Данная тема является весьма актуальной, так как современные информационные технологии позволяют нам упросить контроль над безопасностью на предприятии, и реализовать подобную систему возможно на предприятиях любых масштабов и сфер деятельности. Эти меры позволяют минимизировать ущерб, наносимый организации из-за возникновения непредвиденных чрезвычайных происшествий.

Объектом исследования данной работы является Пенсионный Фонд Российской Федерации.

Предметом исследования является существующая на данный момент интегрированная система охраны в отделении Пенсионного Фонда России по Белгородской области.

Цель исследования – разработка мероприятий по совершенствованию интегрированной системы охраны на предприятии.

Для достижения цели исследования необходимо решить следующие задачи:

1) изучить теоретические аспекты безопасности в организации;
2) исследовать деятельность организации, которой будет предложен комплекс мер, направленных на совершенствование системы охраны;
3) разработать рекомендации по совершенствованию интегрированной системы охраны на предприятии, а также провести оценку эффективности предлагаемых мероприятий.

Используемые методы для разработки и написания данной работы: анализ, сравнения, измерения, системный анализ, моделирование.

Работа состоит из введения, трех глав, заключения и списка использованных источников. В первой главе производится теоретическое исследование предметной области, анализируется рынок интегрированных

систем охраны и их возможности. Во второй главе изучается организационно – управленческая структура организации, анализируется существующая на данный момент система безопасности, проводится анализ ИТ – инфраструктуры организации, выявляются существующие недостатки и предлагаются варианты их устранения. Третья глава исследования включает в себя проект совершенствования интегрированной системы охраны, который состоит в обновлении аппаратного и программного обеспечения существующей интегрированной системы охраны, а также экономическая оценка эффективности предложенного решения. В работе используются схемы, таблицы и изображения. Объем работы – 89 страниц.

1 Теоретические аспекты обеспечения комплексной безопасности на предприятии

1.1 Изучение теоретических аспектов внедрения интегрированных систем охраны в организации

На всех предприятиях создаются безопасные условия труда, устанавливаются правовые основы регулирования отношений между сотрудником и работодателем, а также создаются условия, которые соответствуют требованиям сохранения жизни и здоровья сотрудников в ходе выполнения ими своих должностных обязанностей. Обеспечение таких условий возлагается на руководство предприятия. Цель руководства – создание на базе предприятия такой информационной системы, которая позволит максимально оптимизировать процесс контроля над безопасностью на предприятии. Обеспечение безопасности необходимо для предприятий любых масштабов и сфер деятельности, вне зависимости от форм их собственности, начиная с государственных учреждений и заканчивая магазином розничной торговли. Разница будет лишь в том, в каком объеме, какие методы и средства будут для этого необходимы.

В широком смысле, под понятием безопасность следует понимать состояние защищенности необходимых для функционирования ресурсов предприятия от внутренних и внешних источников опасности.

В узком смысле безопасность предприятия - это такое состояние его правовых, экономических и производственных отношений, материальных, интеллектуальных и информационных ресурсов, которое способствует стабильному функционированию и научно-техническому прогрессу предприятия, как основе эффективной финансово-коммерческой деятельности и условию реализации важнейших социальных интересов

трудовых коллективов дочерних структур и акционерного общества в целом [1].

Целями обеспечения безопасности предприятия являются:

1) выполнение планов производства, обеспечение требуемого качества продукции, активная инвестиционная политика;

2) защита законных прав и интересов предприятия и его сотрудников во взаимоотношениях с государственными органами, партнерами и конкурентами;

3) обеспечение устойчивости порядка внутреннего управления;

4) Обеспечение сохранности и рост собственности предприятия, ее рациональное использование при выполнении производственных задач и удовлетворения потребностей работников предприятия;

5) создание способных к конкуренции товаров и услуг, создание благоприятной рыночной конъюнктуры для их реализации в условиях конкуренции на рынке, рост прибылей предприятия;

6) достижение внутренней и внешней стабильности предприятия, надежности корпоративных связей и недопущение сотрудничества с недобросовестными партнерами;

7) укрепление дисциплины труда и его производительности, формирование стимулов и условий повышения творческой активности сотрудников;

8) полное информационное обеспечение экономической, производственной и научно-технической деятельности предприятия, сохранение коммерческих и государственных секретов, охрана прав на интеллектуальную собственность предприятия.

Конфиденциальная информация различного рода, имеющаяся на любом предприятии, представляет высокий интерес для конкурентов. Если не уделять этой угрозе должного внимания, утечка информации может обернуться большими проблемами для предприятия. Даже единичный случай

безразличного отношения сотрудника к конфиденциальной информации может лишить компанию прибыли и привести к потере доверия клиентов.

Наибольшему риску подвержены такие данные, как данные о составе, статусе и деятельности организации. Источниками угроз являются конкуренты, преступники и коррупционеры. Особую важность представляет доступ к охраняемой информации, а также ее изменение в целях причинения ущерба. Но утечка конфиденциальных данных может произойти и случайно, либо по ошибке сотрудников, либо из-за отсутствия систем защиты информации.

Информационная безопасность организации — целенаправленная деятельность её органов и должностных лиц с использованием разрешённых сил и средств по достижению состояния защищённости информационной среды организации, обеспечивающее её нормальное функционирование и динамичное развитие [2].

Логика функционирования систем информационной безопасности подразумевает прогнозирование и быстрое распознавание угроз безопасности конфиденциальной информации, условий, способствовавших нанесению ущерба предприятию и обусловивших сбои в его работе и развитии, создание рабочих условий, при которых уровень опасности и вероятность нанесения ущерба предприятию сведены к минимуму. Возмещение ущерба и минимизация влияния выявленных попыток нанесения ущерба. Средства защиты информации могут быть:

— техническими;
— программными;
— криптографическими;
— организационными;
— законодательными.

Интегрированная система охраны - это совокупность технических средств различных систем безопасности, реализованных на единой платформе и обеспечивающих автоматическое выполнение заранее

заложенных алгоритмов взаимодействия систем безопасности, а также автоматизацию работы оператора с целью снижения рисков принятия ошибочных решений и уменьшения времени реакции при возникновении внештатной ситуации на объекте [5].

Основой интегрированной системы охраны является единый аппаратно - программный комплекс, представляющий собой автоматизированное управление, имеющий многоуровневую сетевую структуру. Система имеет общий центр, основанный на локальной сети организации, и предусматривает наличие каналов передачи информации, контроллеров различных типов и устройств приема информации. С их помощью комплексные системы безопасности собирают и обрабатывают данные с множества датчиков и контролируют всевозможные средства автоматизации. В такую систему входят система выявления и тушения пожаров, система контроля и управления доступом, система информационной безопасности, система видеонаблюдения за периметром организации.

Перед установкой такой системы, следует понимать, что никакая из подобных систем не будет правильно функционировать без контроля человека. Для надежной и полноценной защиты необходимо подготовить сотрудников организации, которые в обязательном порядке должны соблюдать все предписания по технике безопасности.

Существуют множество классификаций интегрированных систем охраны. Самой простой является разделение, сформированное на основе способов объединения систем безопасности в единый интегрированный комплекс. Согласно этой классификации, существует четыре вида таких систем:

— система с аппаратной интеграцией, которая объединяет системы безопасности при помощи аппаратного обеспечения каждой из них. При таком объединении не используется внешнее программное обеспечение и компьютеры управления. Довольно часто оно осуществляется посредством

релейных контактов. Достоинством такой интеграции является надежность, легкость реализации, а также низкая стоимость. Но такая система не может передавать большое количеств сигналов, и ее сложно изменять;

— система с программной интеграцией, которая действует благодаря специализированному программному обеспечению, установленному на управляющем компьютере. Интегрированная система охраны такого типа может быть построена двумя способами: первый представляет собой специально разработанное программное обеспечение, объединяющее все системы безопасности, а другой способ в качестве интегрирующего программного обеспечения использует программную оболочку одной из систем безопасности. Как правило, это системы контроля доступа;

— система с аппаратно – программной реализацией, в которой не менее трех систем объединены аппаратно и существует компьютер с программным обеспечением, обеспечивающий дополнительный обмен информацией между этими системами, управление ими и сервисные функции. Системы с аппаратно - программной интеграцией имеют те же достоинства, что и системы с программной интеграцией, однако надежность аппаратно – программной интеграции выше, так как при повреждении управляющего компьютера или сбоя в работе программы, комплекс не распадется на отдельные системы, и интеграция сохранится как минимум между тремя системами безопасности. Разработкой систем с аппаратно – программной интеграцией занимается фирма «Болид», ее продукт называется «Орион»;

— интегрированная система охраны с системным программным обеспечением, т.е. система с программной интеграцией, в которой роль интегрирующей программной оболочки выполняет программное обеспечение одной из входящих в комплекс систем безопасности. В таких охранных системах, в большинстве случаев, используется программная оболочка системы контроля и управления доступом. Ее выбор

обуславливается высокой производительностью, в которой уже интегрированы системы охранной сигнализации. Другие системы объединяются программным способом.

Для успешной реализации на предприятии пожарной безопасности, первым делом необходимо установить пожарную сигнализацию. Ее задача – оповещение сотрудников о возможном возгорании. Также можно установить по всему периметру производственных помещений систему автоматического тушения пожара. Также все помещения должны быть снабжены огнетушителями, которые должны располагаться хорошо заметных, доступных местах. Желательно, чтобы сотрудники имели представление о том, как пользоваться огнетушителем до того момента, когда его придется использовать по прямому назначению. И одно из главных правил – это план эвакуации, включающий в себя все входы и выходы, окна, расположение огнетушителей на том или ином этаже, пожарные лестницы, электрощитовые. В практике часто происходят случаи, когда человек в знакомом месте при пожаре, поддавшийся панике, не мог сориентироваться. Правила пожарной безопасности на предприятии для всех одинаковы и должны выполняться в соответствии с требованиями.

Таким образом, в данном разделе были рассмотрены понятия охраны труда, понятие цели безопасности труда, понятие информационной и пожарной безопасности, изучены основные понятия интегрированных систем охраны в целом и их составляющих.

1.2 Анализ рынка интегрированных систем охраны

На рынке присутствует множество организаций, занимающихся разработкой и внедрением интегрированных систем охраны. Их продукция достаточно сильно различается по функционалу и стоимости. Одни организации работают на всероссийском рынке, другие – работают локально.

В квартирах, небольших офисах и магазинах зачастую устанавливают системы видеонаблюдения и сигнализации различного типа. Но на крупных производственных объектах с многочисленным штатом сотрудников необходимо устанавливать интегрированные системы охраны.

Любые технические средства с течением временем устаревают и теряют работоспособность: примерно через 5-10 лет комплекс необходимо будет модернизировать путем замены основных элементов либо всей системы полностью. Поэтому рекомендуется устанавливать все комплектующие от одного производителя, так как это позволит сэкономить средства при эксплуатации.

В Белгородской области присутствует несколько подобных компаний: это общества с ограниченной ответственностью «Стандарт комфорта и безопасности», «Белгородская монтажная компания» и «Контроль и безопасность». Все они присутствуют на рынке достаточно продолжительное время и зарекомендовали себя с хорошей стороны.

ООО "Стандарт Комфорта и Безопасности" представлена на рынке систем безопасности относительно недавно, но ее специалисты имеют большой опыт работы в данной сфере, опыт некоторых специалистов достигает 5-7 лет. Компания ООО «СКБ» сотрудничает с Управлением вневедомственной охраны и Управлением государственного пожарного надзора ГУ МЧС России. ООО "СКБ" представляет полный спектр услуг по построению комплексных систем безопасности, индивидуальному проектированию, монтажу и обслуживанию:

— Цифровых и аналоговых систем видеонаблюдения на объектах любой степени сложности, где необходим видеоконтроль. Доступ к архиву и просмотру видео в режиме онлайн может быть представлен как локально, так и через сеть Интернет;

— Систем охранно-тревожной сигнализации любых объектов, которым требуется защита от несанкционированного доступа в охраняемые помещения;

— Систем противопожарной защиты, в состав которых входят следующие элементы: автоматическая пожарная сигнализация; системы управления эвакуацией людей при пожаре; системы пожаротушения, удаления дыма и вентиляции; огнезащитная обработка конструкций;

— Систем контроля и управлением доступом. Данные системы предназначены для разграничения доступа сотрудников в то или иное помещение охраняемого объекта. Работа системы контроля доступа основана на считывании отпечатков пальцев, кодов Proximity-карточек или брелоков, и дальнейшее принятие системой решения о возможности доступа сотрудника на охраняемую территорию.

Системы контроля и управления доступом данной организации установлены в сети магазинов «Fix Price», ювелирных магазинах «Самоцветы» и «Дива», магазине «Строй – дисконт», коммерческом банке «Альфа – Банк», сети кафе «Додо – пицца» и в Белгородском Индустриальном Колледже.

«Белгородская монтажная компания» - также достаточно серьезная организация на рынке систем контроля и управления доступом. Компания предлагает установку локальных и виртуальных систем наблюдения, охранно – пожарных систем, систем автоматизации производства, систем контроля и управления доступом, занимается установкой дверных домофонов, монтажом структурированных кабельных сетей и проектированием инженерных систем любой сложности. Все системы в дальнейшем поддерживаются, на системы контроля доступа предоставляется гарантия 2 года.

Системы контроля и управления доступом данной компании реализованы на таких крупных предприятиях, как «Белая птица», «Белогорье», молочный завод «Томмолоко», ЗАО Агрофирма «Русь», агропромышленный комплекс «Промагро».

Система контроля и управления доступа включает в себя турникеты, шлагбаумы, считыватели, идентификаторы, замки, объединенные в единый комплекс, что позволяет контролировать территорию объекта, распределять

права доступа и вести базу данных с одного или нескольких компьютеров одновременно. При функциональном расширении связь между передающими и принимающими устройствами может осуществляться посредством IP и GSM технологий.

Компания имеет всю необходимую разрешительную документацию на ведение деятельности по монтажу систем безопасности, а ее сотрудники регулярно проходят аттестацию и курсы повышения квалификации у производителей оборудования.

Одной из лучших компаний по монтажу систем безопасности является «КОДОС». Компания КОДОС — ведущий российский производитель систем безопасности. С 1996 года она осуществляет создание оборудования марки КОДОС, а также сопутствующего программного обеспечения для систем управления доступом. Продукция и программное обеспечение выпускается в тесном сотрудничестве с АО «Бауманн».

Ориентация на потребителя и постоянное совершенствование технологий позволили компании стать надежным поставщиком интегрированных систем охраны. Компания самостоятельно занимается разработкой и поддержкой своей продукции: разрабатываются программная и аппаратная базы, осуществляется производство комплектующих, сертификация, техподдержка, послепродажное обслуживание оборудования и гарантийный ремонт.

«КОДОС» является постоянным участником всех событий в мире безопасности. На протяжении многих лет своей деятельности компания очень хорошо изучила особенности российского и мирового рынков безопасности и была способна предложить собственные актуальные разработки в этой сфере. Благодаря этому продукция «КОДОС» завоевала самые высокие оценки потребителей.

Среди клиентов организации множество крупнейших частных и государственных организаций. Это "ГМК "Норильский никель", Воронежский институт Федеральной Службы Исполнения Наказаний, ООО

«Газпром - бурение», ООО «КамазИнструментСпецмаш», ОАО «Вертолетная сервисная компания», ПАО «АвтоВАЗ» и многие другие.

Также, на всероссийском рынке существует такая компания, как «Болид». Научно-внедренческое предприятие (НВП) "Болид" было основано в 1991. Сфера деятельности предприятия - разработка и поставка оборудования для систем безопасности, автоматизации и диспетчеризации. Производимое оборудование поставляется в страны СНГ и дальнее зарубежье.

На оборудовании НВП «Болид» можно реализовать:

— противопожарные системы: пожарную сигнализацию, оповещение, автоматику пожаротушения и дымоудаления;

— охранные системы: охранно-тревожную и периметральную сигнализацию;

— контроль и управление доступом, управление автотранспортом на парковках;

— охранное видеонаблюдение;

— управление инженерными системами здания;

— учет потребляемых ресурсов;

— мониторинг подвижных объектов.

За последние 15 лет, интегрированная система безопасности «Орион», установлена более чем на 1 млн. объектов и стала самой распространённой в России. "Орион" — пакет программного обеспечения для аппаратно-программного комплекса, на котором реализуются системы охранной сигнализации, контроля и управления доступом, охранного видеонаблюдения, автоматика противопожарных систем, сопряженные с инженерными системами объектов. Программное обеспечение предназначено для организации компьютерных рабочих мест с целью повышения эффективности оперативного контроля и автоматизации управления системами, масштабирования "Орион", построения единых

систем безопасности для территориально распределенных объектов, интеграции всех подсистем на программном уровне.

Среди клиентов компании есть такие крупные торговые сети, как Карусель, Магнит, Лента, Пятерочка, Ашан, коммерческие банки Сбербанк, Россельхозбанк, ВТБ 24 и Бинбанк, Росреестр, Федеральная Налоговая Служба России, Аэропорты Внуково, Сочи, Томск и многие другие.

Как правило, в интегрированные системы охраны входят система контроля и управления доступом, система цифрового видеонаблюдения, системы охранно – тревожной и охранно – пожарной сигнализации, системы сбора и обработки необходимой информации и системы защиты периметра. Также сюда могут входить системы аварийного освещения и гарантированного электропитания, система часофикации и система передачи данных. Работа данной системы осуществляется с помощью системы сбора и обработки информации. Она обеспечивает администрирование, управление и мониторинг различных событий.

Интеграция системы безопасности предоставляет возможность организовать комплексную защиту объектов с централизованным многопользовательским управлением:

— из систем безопасности формируется единая информационная среда, в которую входят система контроля и управления доступом, разветвленная сеть видеомониторинга, система защиты периметра, единая система сбора и обработки информации от всех подсистем;

— задаются алгоритмы взаимодействия систем по соответствующим сигналам друг друга. Так как все подсистемы взаимосвязаны друг с другом, в ответ на сигнал одной из них происходит соответствующее действие в другой;

— интегрированная система охраны позволяет задавать реакции на определенные события. Но решение ключевых вопросов безопасности должно зависеть от человека;

— интегрированная система охраны позволяет оперативно предоставлять руководству достоверные данные о текущей обстановке на подконтрольном объекте;

— предоставляется возможность оперативного оповещения персонала службы безопасности, а также координирование их действий;

— существенно сокращается вероятность ошибочных действий оператора;

— система позволяет выявлять потенциально опасные ситуации, привлекая к ним внимание оператора. Это в свою очередь минимизирует влияние человеческого фактора.

Таким образом, интегрированная система охраны повышает защищенность объекта и заменяет тактику оперативного реагирования на стратегию упреждения угроз. Понять преимущества такой системы будет легче, приведя пример ее действия.

Ранее были выявлены домашние и всероссийские компании – разработчики интегрированных систем охраны, которые являются наилучшими. Проведем обзор возможностей некоторых компаний, работающих на всероссийском рынке.

АРМ Орион Про – это аппаратно – программный комплекс, который позволяет создавать на базе предприятия системы охранно – пожарные сигнализации, системы активной противопожарной защиты (управление пожарной автоматикой, автоматическое тушение возгораний), системы оповещения о пожарах, системы контроля и управления доступом, системы видеонаблюдения и многие другие системы, сопряженные с инженерными системами объектов.

Пакет АРМ "Орион Про" включает в себя программные модули "Сервер", "Администратор базы данных", "Монитор", "Ядро системы", "Оперативная задача", "Генератор отчетов", "Учет рабочего времени", "Видеосервер" и сервисные утилиты. АРМ "Орион Про" способен объединить до 127 локальных ИСО "Орион" одним модулем "Оперативная

задача". В составе АРМ "Орион Про" могут одновременно работать до 63 "Оперативных задач". "Оперативные задачи" имеют 6 исполнений – на подключение 4, 10, 20, 127, 512 и 1024 приборов [6].

Интегрированная система охраны «Орион Про» является более совершенной версией обычного «Ориона», дальнейшее развитие которого прекращено компанией. Система «Орион» поддерживает только базовый функционал систем охранно – пожарной сигнализации и систем контроля и управления доступом. Также «Орион» может работать с существенно меньшим перечнем приборов, в сравнении с «Орион Про».

Помимо поддержки новых приборов, "Орион Про" позволит организовать распределенную систему, в которой каждое из рабочих мест выполняло бы свою конкретную функцию, т.к. данный АРМ имеет клиент-серверную архитектуру ("Орион" предлагает функционал только для одного рабочего места). "Орион Про" может контролировать показания множества устройств: может быть задействовано до 63 компьютера, к каждому из которых возможно подключить до 1024 приборов. В "Орион Про" можно настроить более гибкую реакцию системы на различные события, чем в АРМ "Орион" (пользовательские сценарии с помощью скриптов). В составе АРМ "Орион Про" при покупке "Генератора отчетов" поставляется архитектор отчетов, с помощью которого можно создать любой пользовательский отчет (произвольную выборку по любым параметрам).

Также "Орион Про" имеет уже интегрированную систему видеонаблюдения. Эта видеосистема поддерживает новые модели камер видеонаблюдения, стандарт ONVIF и работает с видеокодеком H.264 с увеличенным количеством камер.

Интегрированная система охраны «Кодос» также предназначена для комплексной защиты объектов от угроз различной природы возникновения и характера проявления. Она также, как и «Орион Про» состоит из системы контроля и управления доступом, охранно – тревожной сигнализации, пожарной сигнализации, системы видеонаблюдения. Но сюда еще входит

подсистема управления электропитания. При необходимости в состав «Кодос» могут включаться продукты других производителей.

Интегрированная система охраны «Кодос» сохраняет свою работоспособность, независимо от работоспособности отдельных частей системы. При выходе из строя отдельных частей системы, оборудование переходит в автономный режим работы с сохранением функционала. Оставшаяся часть системы продолжает функционировать в полном объеме.

Все системы, входящие в «Кодос» функционируют под управлением единого специализированного программного комплекса. Оборудование и программное обеспечение сторонних производителей подключается через модули интеграции. В качестве системы видеонаблюдения в составе «Кодос» может использоваться система видеонаблюдения Axxon Next. Программное обеспечение работает под управлением систем управления базами данных: Firebird, Oracle, MS SQL.

Но нам необходимо выбрать из рассмотренных интегрированных систем охраны одну, которая будет являться наиболее подходящей для отделения Пенсионного Фонда России по Белгородской области. Здание отделения состоит из трех этажей, в нем работает порядка 140 сотрудников, поэтому по размерам можно назвать организацию средней.

Критерием выбора интегрированной системы охраны будет подбор оптимальной для данного объекта совокупности параметров, исходя из критериев подобных систем:

— можно сделать вывод, что рассматриваемый нами объект относится к классу средних;

— на малых и средних по величине объектах нет необходимости задействовать весь функционал интегрированной системы охраны, поэтому желательно использовать системы с модульной архитектурой, чтобы платить только за необходимые в данном конкретном случае функции, а не за всю систему целиком;

— для удобства установки и эксплуатации, система должна иметь интуитивно понятную внутреннюю инфраструктуру с минимально возможным количеством узлов. Центральной частью системы должен являться сервер обработки информации на базе IBM – совместимого компьютера.

ООО «Белгородская Монтажная Компания» специализируется на построении интегрированных систем охраны на крупных предприятиях, что для рассматриваемой в данный момент организации не является предпочтительным. Компании «Кодос» и «Болид» специализируются на системах любых масштабов.

Производители всех интегрированных систем охраны кроме «Стандарт Комфорта и Безопасности» предоставляют возможность приобретения отдельных модулей, что позволяет сэкономить на покупке модулей, которые не будут использоваться.

В открытом доступе стоимость программного обеспечения интегрированных систем охраны указана только на сайтах компаний «Кодос» и «Болид». Для того, чтобы узнать стоимость системы в ООО «Белгородская Монтажная Компания» и ООО «Стандарт Комфорта и Безопасности» необходимо подавать заявку на сайте, и только потом в организацию направляется специалист – оценщик. Осуществить данную процедуру в данный момент не представляется возможным. Если сравнивать цены на продукцию от «Кодос» и «Болид», то второй вариант обойдется дешевле.

Системы безопасности «Кодос» объединяют весь функционал системы на одном компьютере. «Болид» же, благодаря «клиент – серверной» архитектуре, позволяет распределить мониторинг за отдельными частями системы на несколько компьютеров, тем самым разгрузить интерфейс приложения.

Системы охраны от компании «Кодос» работают с оборудованием, которое разрабатывают сами, но также имеется возможность работы с оборудованием от различных производителей, которое будет подключаться

через модули интеграции. Системы охраны «Болид» работают только с собственным оборудованием.

Необходимо также учесть существующую в данный момент систему, точнее ее производителя. Так как в рассматриваемой нами организации уже установлена интегрированная система охраны «Орион», и срок ее действия подходит к концу, наиболее предпочтительным вариантом будет модернизация уже существующей системы в организации до версии «Орион Про». Это позволит упростить процесс обновления, и избежать конфликтов между аппаратным или программным обеспечением.

Таким образом, был рассмотрен местный и всероссийский рынок систем комплексной безопасности. Были рассмотрены возможности, предоставляемые белгородскими компаниями по проектированию и развертыванию подобных систем, а также двумя компаниями всероссийского масштаба. Были изучены основные возможности интегрированных систем охраны, рассмотрена их классификация, выявлены ключевые особенности двух ведущих систем, из которых было отдано предпочтение охранной системе «Орион Про».

2 Анализ существующих в организации технологий организации безопасности

2.1 Изучение деятельности и ИТ–инфраструктуры отделения Пенсионного Фонда России по Белгородской области

22 декабря 1990 года Постановлением Верховного Совета РСФСР создан Пенсионный Фонд РСФСР, ныне Пенсионный Фонд Российской Федерации. Пенсионный фонд Российской Федерации (ПФР) — крупнейшая организация России по оказанию социально значимых государственных услуг гражданам.

ПФР, как государственный внебюджетный фонд, создан для государственного управления средствами пенсионной системы и обеспечения права граждан РФ на пенсию, при этом денежные средства которого не входят в состав федерального бюджета, других бюджетов и фондов к изъятию не подлежат. Бюджет Пенсионного Фонда утверждается Государственной Думой Федерального Собрания РФ отдельным законом вместе с принятием Федерального бюджета России. Доля бюджета ПФР в ВВП России составляет 10,8 % — по доходам, и 10,2 % — по расходам [7].

ПФР – крупнейшая Федеральная система оказания социальных услуг в России. В сферу деятельности ПФР входят:

— установление и выплата пенсий;

— назначение и реализация социальных выплат;

— назначение и реализация федеральной социальной доплаты до уровня прожиточного минимума пенсионера в регионе;

— персонифицированный учет пенсионных прав участников системы обязательного пенсионного страхования;

— формирование и инвестирование средств пенсионных накоплений;

— администрирование страховых взносов на обязательное пенсионное страхование и ОМС;

— выдача сертификатов на получение материнского капитала и выплата средств этого капитала;

— реализация программы государственного софинансирования пенсии;

— оказание адресной помощи пенсионерам и развитие социальной структуры совместно с органами власти.

В состав Белгородского отделения входят следующие структурные подразделения:

— отдел ИТ;

— отдел по защите информации;

— группа по взаимодействию с СМИ;

— группа по ведению делопроизводства;

— отдел организации назначения и выплаты пенсий;

— отдел организации персонифицированного учета и хранения документов;

— управление организации персонифицированного учета, администрирования, страховых взносов и взыскания задолженности;

— отдел социальных выплат;

— отдел казначейства;

— бюджетный отдел;

— группа по актуарным расчетам;

— административно – хозяйственный отдел;

— группа капитального строительства и ремонта;

— отдел организации персонифицированного учета и взаимодействия с страхователями;

— контрольно – ревизионный отдел;

— юридический отдел;

Отдел информационных технологий занимается обеспечением бесперебойного функционирования и развития программно-аппаратных комплексов организации, технической поддержкой средств вычислительной техники и программного обеспечения, работами по оптимизации использования информационно – технических ресурсов организации.

Обязательным условием работы органов ПФРФ является обеспечение конфиденциальности информации, внедрение систем ее постоянной надежной защиты. Для этих целей был создан отдел по защите информации, который занимается комплексной защитой информации, с которой работает организация. С 2003 года в Отделении и районных Управлениях ПФР установлена система шифрования трафика, введено новое программное обеспечение. Сегодня работники отдела успешно реализуют многочисленные проекты: проведена работа по созданию защиты автоматизированной информационной системы отделения ПФР, защищенного электронного документооборота, антивирусной защиты.

Группа по взаимодействию с СМИ занимается информационным представительством организации в муниципальных и государственных органах, а также взаимодействует со средствами массовой информации для информирования жителей о важнейших событиях в деятельности организации.

Управление организации назначения и выплаты пенсий можно отнести к сложным структурным органам и отделениям ПФР. Главная задача его сотрудников - точный и своевременный перерасчет пенсий тем, у кого изменились размеры выплат, и назначение ее гражданам, которым выплата только была назначена. Все операции с деньгами проводятся строго в соответствии с законодательством, действующим на территории России. Помимо пенсий в функции отдела входит выплата различных социальных пособий гражданам, входящим в различные льготные категории.

Отдел социальных выплат специализируется на распределении пособий, оказании материальной помощи гражданам, которые по каким – либо причинам оказались в тяжелом материальном положении. Также отдел осуществляет оформление различных документов. Например, удостоверений многодетным семьям, оформление материнского капитала.

В функции отдела казначейства входят проведение различных платежей, привлечение денежных средств при их дефиците, управление различными рисками и их координация в рамках централизованного управления активами и пассивами организации.

Контрольно - ревизионный отдел осуществляет внутренний финансовый надзор, занимается проверкой деятельности структурных подразделений, качества бухгалтерского учета и принимает меры по устранению выявленных нарушений или недостатков.

И, наконец, юридический отдел обеспечивает соблюдение законности деятельности организации, регулированием экономических отношений, выявляет и устраняет правонарушения и занимается их профилактикой.

Далее был проведен анализ ИТ – инфраструктуры отделения Пенсионного Фонда России по Белгородской области. ИТ – инфраструктурой называются все аппаратные и программные средства, с помощью которых возможно управлять, собирать, обрабатывать, хранить информацию. Если не уделять должного внимания этой сфере, то в конечном итоге искаженные данные или сведения о деятельности компании могут нанести огромный вред. [15]

Правдивая информация, предоставленная в полном объеме, высокая скорость ее получения и информационного обмена между структурными подразделениями организации играет огромную роль для рентабельности и конкурентоспособности предприятия. Все это становится важным фактором для принятия решения о том, что компания имеет эффективный вектор развития в сфере информационных технологий и всей бизнес-структуры в целом.

Структурно анализ ИТ инфраструктуры подразделяется на четыре составных части. Это компьютерная составляющая, система безопасности, автоматизации и коммуникационных сетей. Для принятия решения о том, что анализ информационной системы действительно будет проводиться эффективно, понадобятся две составляющие. Это полезная эффективность и информационная безопасность. Чтобы обеспечить и первый, и второй аспект, необходимо проводить специальные исследования деятельности организации, что и подразумевает под собой анализ ИТ. Он обеспечивает оптимизацию информационной системы. Аудит для эффективного управления компанией и использования всех ее системных ресурсов – это самый лучший способ выявить все явные и скрытые варианты рисков инфраструктуры организации [15].

Результатом анализа ИТ – инфраструктуры организации должны стать:

— актуальная оценка текущего её состояния;

— объем существующих и потенциальных ресурсов;

— информация о сильных и слабых сторонах ее составляющих элементов

— рекомендации по ее оптимальному использованию и необходимой модернизации [16].

Отделение Пенсионного Фонда России по Белгородской области располагается на трех этажах достаточно крупного здания. Для поддержания информационных связей между подразделениями и их работниками создается локальная вычислительная сеть [17].

Локальная вычислительная сеть (ЛВС) организована при помощи выделенной линии Интернет, маршрутизатора, брандмауэра, коммутатора, серверов, и рабочих станций. Она позволяет совместно использовать различные устройства, подключенные к сети, такие, как рабочие станции, сканеры, принтеры, плоттеры, модемы, и прочие периферийные устройства. Компьютеры расположены в пределах одного здания и соединены при

помощи скоростных линий связи со скоростью обмена данными не менее 100 Мбит/с (не исключается случаи соединения компьютеров и с помощью низкоскоростных телефонных линий).

Знание топологии сети позволяет определить её слабые места для их последующего устранения. Также зная все недостатки в схеме сети, можно учесть их при подключении нового сетевого оборудования и рабочих станции [19].

В отделе по защите информации, где мною было занято одно из рабочих мест, используется 6 компьютеров, принтер и 5 телефонов, подключенных через интернет общей сети. Все компьютеры равнозначны, и подключены к серверу организации. Телефоны подключены через канал связи к компьютерам, они необходимы для осуществления разговоров по соответствующим отделу вопросов с другими организациями. На рисунке 2.1 изображена схема подключения компьютеров.

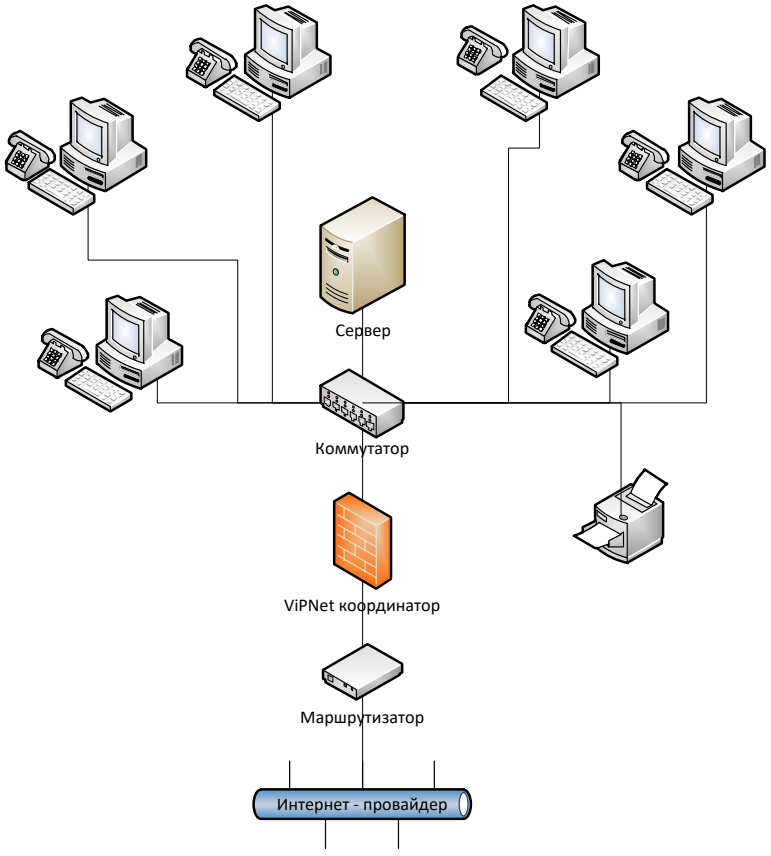

Рисунок 2.1 – Топология локальной сети отдела по защите информации

В организации реализована топология сети Звезда. В этом случае каждый компьютер подключается отдельным кабелем к общему устройству - свитчу (коммутатору), который связан с роутером. С помощью сервера ведётся централизованное управление всей сетью, определяются маршруты передачи сообщений, подключаются периферийные устройства. Также сервер является хранилищем данных всей сети.

Достоинства топологии «звезда»:

— выход из строя одной рабочей станции или повреждение ее кабеля не отражается на работе всей сети в целом;

— отличная масштабируемость;

— легкий поиск и устранение неисправностей и обрывов в сети;

— высокая производительность;

— простота настройки и администрирования;

— в сеть легко встраивается дополнительное оборудование [18].

Стоит отметить, что иногда возникают перебои в подаче электричества на объект. Помимо прекращения функционирования локальной сети, появляется вероятность утери различной информации с серверов (например, данные системы контроля и управления доступом).

В отделе по защите информации используется 6 компьютеров, принтер и 5 телефонов. В таблице 2.1 представлены данные об аппаратном обеспечении данного отдела

Таблица 2.1 – Аппаратное обеспечение отдела по защите информации.

Должность	**Аппаратное обеспечение**
Начальник отдела	Компьютер, принтер, телефон
Главный специалист – эксперт	Компьютер, принтер, телефон
Ведущий специалист - эксперт	Компьютер, принтер, телефон
Ведущий специалист - эксперт	Компьютер, принтер, телефон
Ведущий специалист - эксперт	Компьютер, принтер, телефон

В каждом из отделов организации аппаратное обеспечение схоже. Различаются только количество оборудования, и его технические характеристики.

Аппаратное обеспечение рабочих мест рассматриваемой организации представлено в таблице 2.2

Таблица 2.2 – Аппаратное обеспечение рабочих мест организации

Рабочая станция		**Количество**
Процессор	Intel Core 2 Duo, 2.66 ГГц\Intel Core i3 2.3 ГГц	**100**
Материнская плата	ASRock ConRoeXFire-eSATA2	
Видео плата (карта)	Nvidia GTS 230	
Звуковая плата(карта)	Realtek ALC887	
Блок питания	300Вт	
Жесткий диск	320 Гбайт – 1 Тбайт	
ОЗУ	4 Гб DDR2	
Монитор	ЖК 19" Samsung SyncMaster 19C150N	
Клавиатура	Genius KB-06X, PS/2	
Мышь	Genius NetScroll 110	
Телефонные аппараты		**140**
Телефонный аппарат	Yealink SIP-T19 E2	140
Принтеры и копировальная техника		**15**
Принтер струйный	HP Deskjet 1015 (B2G79C)	3
Принтер лазерный	Samsung ML-2165	4
Принтер лазерный	HP LaserJet P1102	3
МФУ	HP Color LaserJet Pro M377dw	5

Морально-устаревшие компьютеры составляют 40 % от общего числа. Данная проблема замедляет работу сотрудников.

Отдел по защите информации использует, лицензионное программное обеспечение, к которым относят офисный пакет приложений, корпоративные приложения и ресурсы, приложения нормативно-правовой поддержки.. Перечень программного обеспечения, используемого в отделе по защите информации представлен в таблице 2.3

Таблица 2.3 – Программное обеспечение отдела по защите информации.

Вид программного обеспечения	**Название программного обеспечения**
Операционная система	Windows 7 Professional
Браузер	Internet Explorer, Mozilla Firefox
Почтовый клиент	IBM Lotus Notes
Офисный пакет	Microsoft Office 2010 Pro
Работа с паролями	SSO Indeed Enterprise
Антивирус	Kaspersky
Нормативно-правовая поддержка	Консультант Плюс

Отдел по защите информации Отделения Пенсионного Фонда России по Белгородской области занимается администрированием и обеспечением безопасности порядка 50 корпоративных информационных ресурсов. Эти ресурсы содержат информацию ограниченного доступа, не содержащую сведения государственной тайны.

Таким образом, была рассмотрена деятельность каждого из структурных подразделений отделения Пенсионного Фонда России по Белгородской области. Был проведен анализ ИТ – инфраструктуры отделения, в ходе которого были выявлены следующие уязвимые места:

— редкие перебои с подачей электропитания;

— использование морально устаревшей техники;

— использование не актуальных версий программных продуктов.

Рекомендуется установить дизель – генераторную установку для обеспечения бесперебойного питания административного здания, а также установить ИБП для питания свитчей и маршрутизаторов.

2.2 Анализ существующей в организации системы безопасности

На данный момент в Белгородском отделении Пенсионного Фонда внедрена интегрированная система охраны «Орион». Она контролирует работу системы учета рабочего времени и охранно – пожарной системы. Версия программного обеспечения данной системы уже морально устаревает, и компания – производитель уже не выпускает для нее обновления ПО, осуществляя только техническую поддержку.

Система «Орион» - объектно - ориентированная система, предназначенная для организации рабочего места дежурного оператора службы охраны и управления работой следующих подсистем: охранная и пожарная сигнализации, контроль доступа, управление пожарной автоматикой.

Программное обеспечение системы устанавливается на IBM совместимую электронно - вычислительную машину и работает под управлением ОС Windows. Для каждого компьютера необходимы мышь и звуковая карта. Рекомендуемый размер экрана от 19 до 21 дюйма (на некоторых компьютерах используют по два совмещенных монитора).

Подключение устройств происходит через COM-порты и преобразователь интерфейсов с гальванической развязкой (ПИ-ГР), или преобразователь интерфейсов с автоматическим переключением направления передачи i7520.

Состав программного обеспечения системы «Орион» состоит из множества программ - подсистем:

— «Оперативная задача» - предназначена для ведения журнала событий (опроса подключенных приемно – контрольных приборов), управлением взятием или снятием охраны объекта, контроля и графического отображения состояния подконтрольных зон, речевого оповещения сотрудников организации об возникшей чрезвычайной ситуации;

— «Администратор базы данных» - управляет вводом, редактированием, сортировкой и обменом данными, необходимыми для правильного функционирования всего охранного комплекса;

— «Генератор отчетов» - формирует отчеты о состоянии и событиях аппаратной части охранного комплекса в выбираемый пользователем промежуток времени;

— «Мастер системы» - позволяет архивировать, удалять и восстанавливать информацию, внесенную в базу данных системы. Не работает с приборами и контроллерами;

— «Uprog» - утилита для настройки конфигурационных параметров приборов;

— «Shleifes» - утилита, показывающее текущее состояние шлейфов всех подключенных к системе приборов в реальном времени путем запроса значений АЦП и вычисления на основе этих данных сопротивлений шлейфов этих приборов;

— «Редактор планов» - позволяет прорисовать план помещений организации;

— «Демонстратор» - предназначен для эмуляции работы приборов, занесенных в базу данных системы;

— «Учет сотрудников, находящихся на объекте» - контролирует нахождение сотрудников организации на своих рабочих местах;

— Сетевой «Учет рабочего времени» - утилита для вывода отчетов по учету рабочего времени;

— «Сервер базы данных» - сервер, необходимый для работы с базой данных программ «Учет рабочего времени» и «Учет сотрудников, находящихся на объекте»;

— «Конфигурирование пульта С2000» - программа конфигурирования пультов;

— «Удаленный мониторинг за персоналом» - программа для сетевого мониторинга карточек сотрудников, приходящих на объект.

Оператор системы «Орион» работает непосредственно с «Оперативной задачей» системы и должен использовать следующие команды и функции данной программы:

— запуск программы и идентификация оператора;

— смена дежурства;

— постановка на охрану и снятие с охраны зон и разделов;

— обработка тревог;

— запуск сценариев управления;

— управление элементами контроля доступа;

— отображение статистики и регулирование порогов задымленности, запыленности;

— запуск хранителя экрана;

— отключение тревожного звукового оповещения;

— просмотр списка подключенных приборов;

— загрузка информационных карточек;

— просмотр статуса программы;

— переключение между планами помещений;

— получение отчета за смену;

— штатное завершение работы программы.

На входе в отделение имеется пост охраны, на котором установлен сервер, необходимый для работы всей охранной системы. Сотрудники проходят на свои рабочие места через единственный турникет, который также установлен на посту охраны. Идентификация сотрудников происходит с помощью электронных пропусков, к каждому из которых присвоен индивидуальный номер. Каждое использование такого пропуска отображается в системе. На входе в помещения, в которых осуществляется обработка персональных данных, также установлены считыватели пропусков. Это позволяет разграничить доступ сотрудников к помещениям организации. Сотрудники, у которых нет электронного пропуска (посетители отделения, работники организаций, осуществляющих техническое обслуживание оргтехники и т.д.), получают временный пропуск, действующий до момента ухода этого человека с объекта.

У существующей в организации системы охраны существуют недостатки. Так, например, рабочий день в организации начинается в 8 часов и 30 минут. Если сотрудник придет на работу раньше 8 часов, то система может вообще не увидеть его, а если он покинет здание пенсионного фонда в временном промежутке с 8 часов до 8 часов и 30 минут, то система запишет

этому сотруднику опоздание на работу. Ввиду отсутствия обновлений системы, программное обеспечение периодически зависает.

Еще одной проблемой является отсутствие подключения сервера АРМ «Орион» к источнику бесперебойного питания. Это делает сервер интегрированной охранной системы зависимым от перебоев в подаче электричества. Если такое случается, все данные из базы могут быть утеряны. Чтобы этого избежать, организовано один раз в неделю создание резервных копий базы данных.

Также, к недостаткам можно отнести прокси – карты. Они являются недолговечными и быстро приходят в негодность. Решением данного недостатка может стать замена считывателей прокси – карт на новые, которые будут поддерживать распознавание технологии Near Field Communication (NFC). Помимо использования NFC – брелоков, можно привязать к системе контроля и управления доступом NFC – модуль смартфона (при наличии его в смартфоне сотрудника), и отказаться от физических пропусков вовсе.

Система пожарной безопасности включает в себя системы автоматического пожаротушения, датчики дыма и высоких температур, систему звукового оповещения сотрудников о возникновении пожара в организации. Данные с датчиков обрабатываются и отображаются на пульте, находящемся на посту охраны.

Система охраны включает датчики открытия на дверях и окнах. В случае, если объект поставлен на охрану, то при попытке проникнуть в здание включается сирена, и соответствующий сигнал поступает на пульте, находящемся на посту охраны. Также на дверях помещений, с ограниченным доступом (в которых происходит обработка персональных данных) установлены магнитные замки, которые открываются от электронного пропуска. Сотрудники, находящиеся в кабинете, имеют возможность открывать эти замки изнутри.

Для выявления уровня условий труда и уровня функциональности существующей на данный момент интегрированной системы охраны были проведены исследования с помощью следующих методик:

— метод фокус-группы;

— SWOT – анализ;

— построение диаграмм «Как есть» и «Как должно быть».

Фокус – группа – качественный метод, который заключается в сборе определенной группы людей, порядка 8-10 человек, для обсуждения некоторой темы, в которой каждый из участников группы заинтересован, в той или иной степени. Обсуждение продолжается до двух часов, но нередко возникает такая ситуация, когда обсуждение затягивается на гораздо больший срок. Дискуссии при таком собрании относятся к технологиям качественного анализа, так как информация, которая получается в результате работы таких специалистов, не может называться репрезентативной для определенной группы людей [7].

Также фокус-группа – это эффективный инструмент для понимания скрытых побуждений и мотивов касательно уровня обслуживания. У участников всегда есть различная информация, которая получена на основе собственного жизненного опыта, касательно высокого и низкого уровня обслуживания, и в отличие от преимущественного большинства других тем потребитель радостно обсуждает эту информацию с другими людьми. Таким образом, фокус-группа – это довольно популярный вариант проникновения в самые разные аспекты качества обслуживания, а также уровня удовлетворенности и постоянства со стороны потребителей.

Цель проводимого исследования заключалась в выявлении степени удовлетворенности сотрудников Белгородского отделения Пенсионного Фонда России организацией безопасности труда. Задачей исследования стало рассмотрение такого аспекта, как степень удовлетворенности сотрудниками существующими на данный момент мерами безопасности.

Была собрана фокус – группа, в которой в качестве респондентов выступали 6 человек. В группе участвовали 6 сотрудников Белгородского отделения Пенсионного Фонда России, работающих в различных отделах. Из них – 3 мужчины и 3 женщины в возрасте от 25 до 48 лет. Продолжительность фокус – группы составила 1 час. Сотрудники были проинструктированы о правилах проведения этого исследования. В соответствии с поставленными задачами был составлен перечень вопросов, получив ответы на которые можно понять, насколько сотрудники удовлетворены существующей обстановкой в сфере безопасности труда.

Были использованы следующие вопросы:

1) Какие меры по обеспечению безопасности труда, проводимые руководством организации, вы можете назвать? Устраивают ли они вас в целом?

2) Как вы считаете, какие условия в области организационно – технической безопасности должна предоставлять компания своим сотрудникам? Устраивают ли вас существующие в организации на данный момент условия труда?

3) Что должен делать работодатель для обеспечения санитарно – гигиенических и лечебно – профилактических мер безопасности? Обеспечиваются ли в вашей организации должные условия?

Таким образом, в результате беседы с сотрудниками выяснилось, что сотрудники удовлетворены условиями безопасности и охраной труда в организации. Исследование можно назвать успешным.

Также, был проведен SWOT – анализ. Это метод стратегического планирования, заключающийся в выявлении факторов внутренней и внешней среды.

Таблица с SWOT – анализом системы охраны и условий охраны безопасности труда представлена в таблице № 2.4

Таблица 2.4 – SWOT - анализ

Strengths (сильные стороны)	**Weaknesses (слабые стороны)**
Наличие у всех сотрудников индивидуальных средств защиты;	Монотонная и однообразная работа;
Очень низкая вероятность получения травм на производстве;	Низкое качество мониторов рабочих компьютеров
Высокая квалификация сотрудников.	
Opportunities (возможности)	**Threats (угрозы)**
Возможность автоматизации некоторых процессов;	Неправильная организация рабочего места;
Рост доходов населения;	Наличие морально устаревшего или поврежденного оборудования и технологий;
Возможность модернизации оборудования.	Наличие легковоспламеняющихся материалов на рабочих местах.

Таким образом, с помощью SWOT – анализа мы выявили следующие проблемы:

1) риск ухудшения зрения сотрудников вследствие использования мониторов с низким качеством изображения;

2) некоторые средства индивидуальной защиты либо просрочены, либо хранятся по другому адресу;

3) некоторые сотрудники не умеют пользоваться средствами индивидуальной защиты.

Также были построены диаграммы «Как есть» и «Как должно быть». В качестве примера был рассмотрена ситуация с возгоранием. В данный момент все происходит следующим образом: активная система собирает данные с датчиков температуры и дыма. Если полученные показатели превышают заранее заданные значения, поступает сигнал на пульт охраны, включается пожарная тревога. Далее, если факт возгорания подтверждается, оповещаются экстренные службы и активируется система пожаротушения. Схема данного процесса «как есть» представлена на рисунке 2.2.

После проведения модернизации интегрированной системы охраны в Белгородском отделении Пенсионного Фонда России, все будет происходить следующим образом. После срабатывания системы пожарной сигнализации, система видеонаблюдения выведет на монитор изображение от ближайших к месту возникновения пожара видеокамер. Полученное изображение автоматически анализируется интегрированной системой охраны на наличие дыма или открытого огня. При подтверждении возгорания, интегрированная система охраны согласно заданному сценарию формирует команды, которые будут исполняться другими подсистемами. Система контроля доступа откроет эвакуационные выходы. Дым вдоль маршрутов эвакуации будет удален подсистемой дымоудаления. Автоматически будет включена система аварийного освещения. Вышеописанный сценарий возможен благодаря взаимодействию отдельных систем комплекса. Схема процесса «Как должно быть» представлена на рисунке 2.3

Таким образом, была рассмотрена существующая система охраны в Белгородском отделении Пенсионного Фонда России. Выявлены особенности и недостатки работы существующей системы. Также был проведен анализ методом «фокус – группы», которая выявил удовлетворенность сотрудников организацией безопасных условий труда, проведен SWOT – анализ, который выявил слабые стороны существующей на данный момент организации безопасности. И, наконец, были построены диаграммы «как есть» и «как должно быть» процесса «возникновения возгорания». Ввиду отсутствия поддержки от производителя и морального устаревания рекомендуется запланировать работы по модернизации существующей системы. Рекомендуется замена всех устаревших и плохо функционирующих элементов системы безопасности, обновление программного обеспечения системы до актуальной версии и модернизация парка персональных компьютеров.

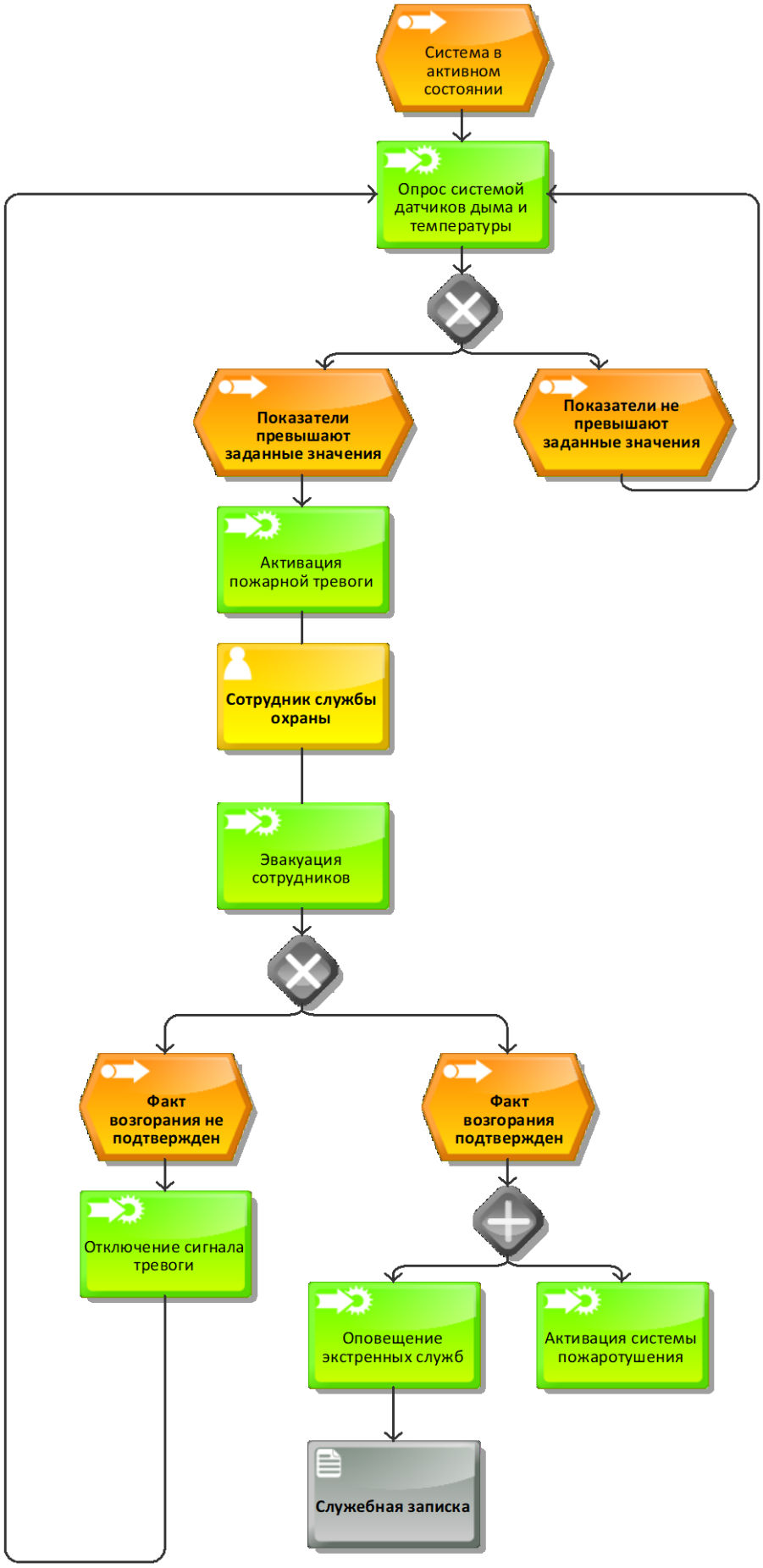

Рисунок 2.2. – Диаграмма «Как есть» процесса «Возникновение пожара»

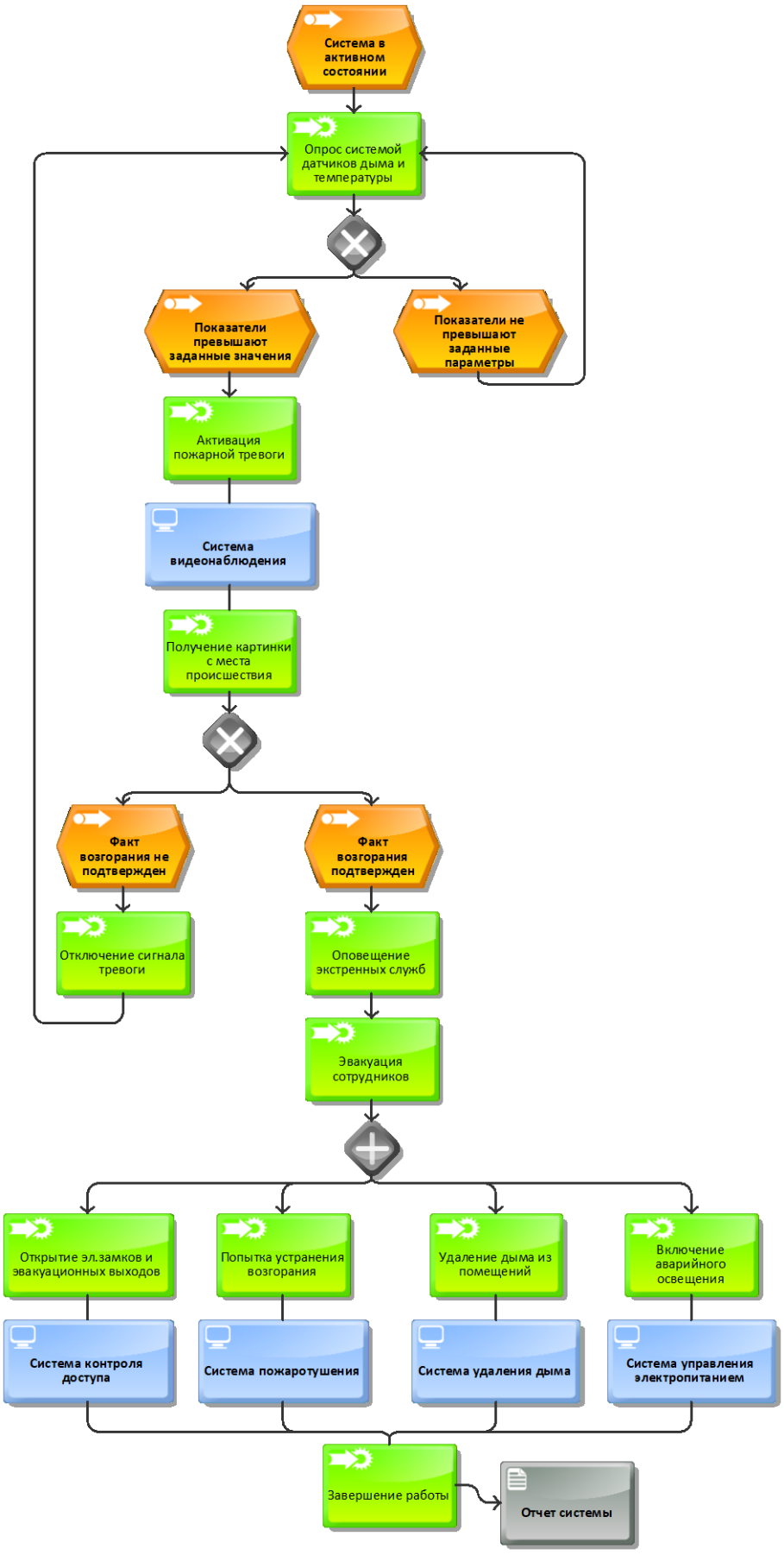

Рисунок 2.3 – диаграмма «Как должно быть» процесса «Возникновение пожара»

3 Разработка проекта модернизации существующей интегрированной системы охраны

3.1 Выработка рекомендаций по совершенствованию интегрированной системы охраны Отделения Пенсионного Фонда России по Белгородской области

Для систематизации и координации всех действий по совершенствованию интегрированной системы охраны отделения Пенсионного Фонда России необходимо разработать техническое задание. Полный текст технического задания представлен в приложении к выпускной квалификационной работе.

В предыдущей главе были представлены и проанализированы методики, которые позволили выявить ряд актуальных проблем на предприятии:

1) несоответствие характеристик существующей локальной сети современным требованиям;
2) моральное устаревание программного и аппаратного обеспечения существующей системы охраны;
3) низкая производительность рабочих компьютеров.

Техническое задание (ТЗ) — документ, содержащий в себе требования заказчика к объекту закупки, определяющие условия и порядок ее проведения для обеспечения государственных или муниципальных нужд, в соответствии с которым осуществляются поставка товара, выполнение работ, оказание услуг и их приемка [9].

Создание технического задания выступает одним из первых и чрезвычайно важных этапов большинства проектов. Правильно составленное техническое задание позволяет внести ясность в отношения заказчика и исполнителя, четко сформулировать требования к характеристикам будущего

объекта, а также становится основанием для проверки выполненной работы [10].

Чтобы облегчить составление и выполнение технического задания, его разрабатывают по определенной системе. В вводной части, излагают цель и назначение проекта. Далее следует перечисление разделов, требований и их расшифровка. Чтобы понять, как выглядит ТЗ для автоматизированной системы, можно рассмотреть структуру, рекомендуемую ГОСТом 34.602-89:

— Указание общих сведений.

— Описание назначения и цели, ради достижения которой планируется создание или развитие системы.

— Характеристики объектов, подлежащих автоматизации.

— Изложение требований к системе.

— Состав и содержание мероприятий и работ, применяемых для создания системы.

— Описание того, как должен проходить контроль создания и процедура приемки готовой системы.

— Перечень требований к работам, которые будут проводиться с объектом автоматизации для его подготовки.

— Порядок ведения документации.

— Указание источников разработки [22].

Настоящим техническим заданием предусмотрено выполнение работ по модернизации интегрированной системы охраны, используя технические средства материалы (изделия и конструкции) приобретаемые за счет исполнителя государственного контракта. Полный текст технического задания на модернизацию интегрированной системы охраны отделения Пенсионного Фонда России по Белгородской области представлен в приложении.

В рамках проекта автоматизируется деятельность предприятия в следующих процессах:

1) разграничение и контроль доступа;

2) обеспечение физической безопасности на предприятии;

3) обеспечение противопожарной безопасности;

4) обеспечение защиты конфиденциальной информации, имеющейся в организации;

5) контроль периметра организации;

6) Составление итоговых отчетов о работе системы.

ИСО ОПФР по Белгородской области модернизируется с целью:

— повышения качества выполняемых системой функций;

— сокращения времени на выполнение заложенных в систему сценариев;

— упрощения работы для службы безопасности.

Основные процессы, подлежащие модернизации приведены в таблице 3.1

Таблица 3.1 – Основные процессы

Наименование процесса	Возможность автоматизации	Решение об автоматизации в ходе проекта
Контроль и управление доступом	Возможна	Будет модернизирован
Физическая безопасность на объекте	Возможна	Будет модернизирован
Пожарная безопасность	Возможна	Будет модернизирован
Защита конфиденциальной информации	Возможна	Будет модернизирован
Охрана периметра объекта	Возможна	Будет модернизирован
Учет рабочего времени	Возможна	Будет модернизирован

Система контроля и управления доступом должна обеспечивать санкционированный доступ должностных лиц в помещения административного здания ОПФР по Белгородской области, препятствовать

несанкционированному проникновению или попыткам проникновения на охраняемый объект посторонних лиц, а также:

— идентификацию персонала и управление доступом в помещения;

— учет рабочего времени должностных лиц.

Холл ОПФР по Белгородской области должен быть оборудован турникетом с бесконтактным дистанционным считывателем, а также полуростовыми ограждениями зоны ожидания с калиткой для проезда инвалидных колясок

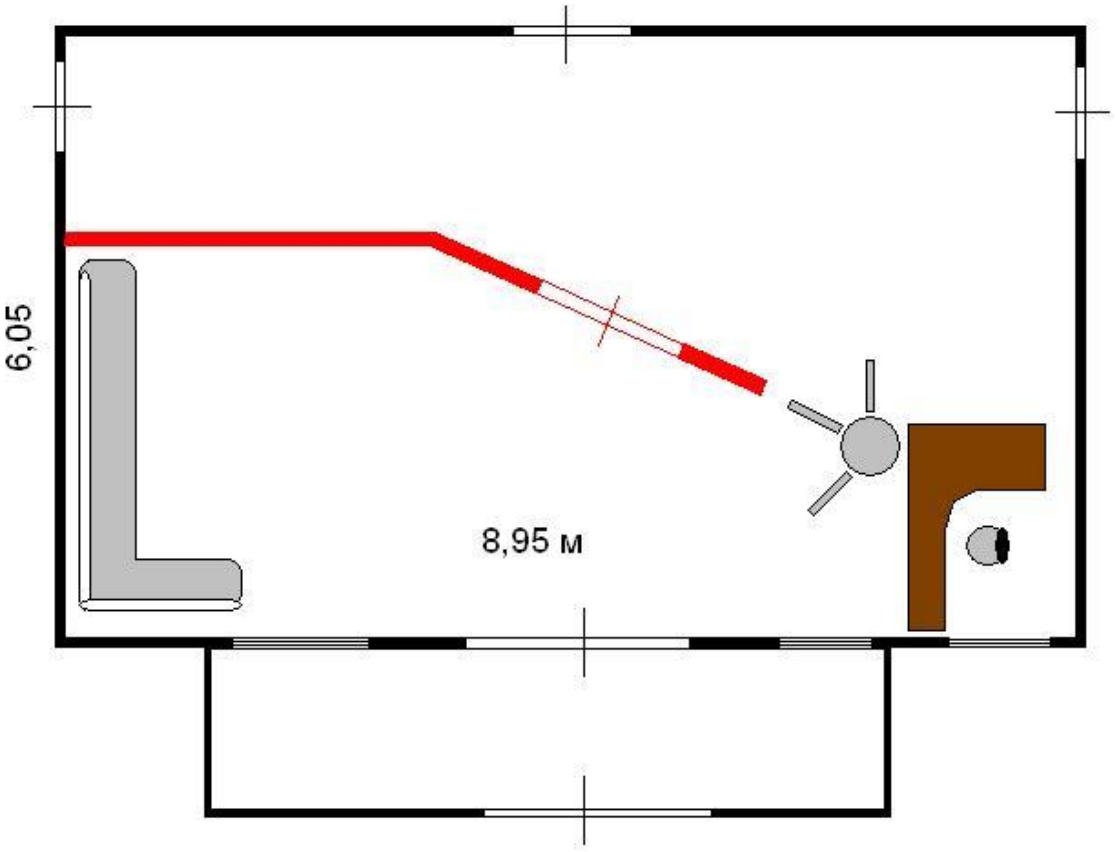

Рисунок 3.1 – План холла в ОПФР по Белгородской области

Каждый контролируемый проход должен быть оборудован бесконтактными дистанционными считывателями, замковыми устройствами.

Размещение системы должно отвечать требованиям:

— аппаратура, входящая в состав СКУД, должна быть выполнена в блочном исполнении;

— считыватели устанавливаются в коридорах здания.

Средствами системы контроля и разграничения доступа оборудуются помещения ограниченного доступа (в которых производится обработка персональных данных), где должно быть исключено несанкционированное пребывание посторонних лиц. Помещения должны быть постоянно закрытыми и запертыми.

Открывание замка для входа в указанные помещения обеспечивается дистанционными считывателями смарт-карт. Отпирание замка для выхода из помещения осуществляется нажатием специальной кнопки.

Обеспечение электроснабжением системы должно соответствовать требованиям СНиП 2.04.09-84 и РД 78.143-92. Электропитание комплексной системы безопасности должно обеспечиваться по первой категории.

Система бесперебойного питания строится по распределённой схеме и должна обеспечить выполнение следующих функций:

— автономное электропитание оборудования СКУД при отсутствии напряжения в сети переменного тока;

— защиту активного сетевого оборудования от импульсных помех внешней электросети и от перенапряжения;

— поддержание максимальной ёмкости аккумуляторных батарей при наличии сети переменного тока;

— Устанавливаемые на объекте ИБП должны отвечать требованиям ГОСТ 27699-88 и ГОСТ Р 50745-95 и:

— работать в широком диапазоне изменения входного напряжения (не менее+15%);

— иметь значение коэффициента входной мощности близкое к единице;

— коэффициент гармонических искажений на входе не более 8%;

— иметь КПД не ниже 92-94%;

Электрические проводки должны подразделяться на:

— линии связи (шлейфы сигнализации, цепи управления, шины данных, интерфейсные шины);

— низковольтные цепи питания (12/24 В постоянного тока);

— высоковольтные цепи питания (220/380 В переменного тока частотой 50 Гц).

Проектирование линий связи и низковольтных цепей питания должно осуществляться с учетом требований ПУЭ, СНиП 3.05.06-85. Выбор кабелей и проводов производить с учетом их технических характеристик. Прокладка данных цепей должна производиться: скрыто в штробе; в лотках за подвесными потолками, в трубах ПВХ, в электротехническом коробе.

Защитное заземление или заземление технических средств должно соответствовать ПУЭ, СНиП 3.05.06-85, ГОСТ 12.1.030-81 и технической документации на аппаратуру СКУД.

Для обеспечения эксплуатация интегрированной системы охраны необходимо выделить 1 сотрудника, который будет работать с АРМ системы. Это должен быть уверенный пользователь ПК, с навыками работы с приложениями операционной системы Windows, а также имеющий навыки системного администратора.

Система подвергается испытаниям следующих видов:

1) предварительные испытания;
2) опытная эксплуатация;

— приемочные испытания.

Состав, объем и методы предварительных испытаний системы определяются документом «Программа и методика испытаний», разрабатываемым на стадии «Рабочая документация».

Таблица с приведенным перечнем работ, необходимым оборудованием, материалами и программным обеспечением представлена в приложении к техническому заданию.

Также, по результатам проведения анализа ИТ – инфраструктуры отделения Пенсионного Фонда России по Белгородской области были выявлены следующие недостатки:

— перебои в работе локальной сети, вызванные использованием устаревшего сетевого оборудования;

— редкие перебои с подачей электропитания;

— низкая производительность персональных компьютеров;

— использование неактуальных версий программных продуктов.

Выявленные недостатки достаточно серьезно влияют на производительность труда, а также являются угрозой для нормального и бесперебойного функционирования интегрированной системы охраны, и их необходимо устранить.

В первую очередь, необходимо заменить сетевое оборудование. Существующие на данный момент кабели локальной сети не соответствуют современным технологиям обработки информации, рекомендуется заменить на новые. По предварительным подсчетам, необходимо заменить порядка 1000 метров кабеля.

Также, необходимо решить проблему с перебоями в подаче электричества. Рекомендуется установить дизель – генераторную установку, которая обеспечит бесперебойную подачу электропитания в административное здание отделения. Каждый компьютер и сервер в организации необходимо оснастить источником бесперебойного питания на случай отключения основного электропитания. Это позволит обеспечить бесперебойную работу интегрированной системы охраны, а также работу отделения Пенсионного Фонда в целом, и предотвратит утерю ценных для организации данных.

Далее, была выявлена неудовлетворительная производительность персональных компьютеров, в том числе и текущего АРМ интегрированной системы охраны. Это вызывает проблемы в работе программного обеспечения самой системы безопасности. Рекомендуется обновить аппаратное обеспечение организации. Примерный состав сборки новых компьютеров представлен в таблице 3.2

Таблица 3.2 – Рекомендуемая сборка персональных компьютеров для организации

Рабочая станция		**Количество**
Процессор	Intel Core i3-7100 3.9 ГГц	**50**
Материнская плата	MSI H110M PRO-VDP	
Видеоплата (карта)	Asus GeForce GT 1030 Silent LP	
Звуковая плата(карта)	Встроена в материнскую плату	
Блок питания	Aerocool VX-550, 550 Вт	
Жесткий диск	Seagate 5900 IronWolf 1 Тб	
ОЗУ	Qumo [QUM4U-4G2133KK15] 4 ГБ	
Монитор	ЖК 21.5" AOC E2270SWHN	
Клавиатура	Sven Standart 307M	
Мышь	Sven RX-180	

Стоимость сборки одного такого компьютера составит порядка 45 тысяч рублей. Замена части устаревших компьютеров на такую сборку позволит существенно повысить производительность труда, а также упростит контроль за безопасностью на предприятии.

Также, сотрудники организации работают с устаревшим программным обеспечением. Рекомендуется полностью отказаться от программного обеспечения 1С версий 7.х. Данные программные продукты медленно работают, и не имеют удобного функционала более свежих версий. Также, многие компьютеры работают на устаревших версиях операционной системы, а именно Windows XP и Windows 7. Поддержка Windows XP прекращена уже давно, а поддержка Windows 7 будет прекращена в 2020 году.

Таким образом, в данном разделе было начато составление технического задания, которое станет основополагающим документом, регулирующим все планируемые работы по совершенствованию интегрированной системы охраны в отделении Пенсионного Фонда России

по Белгородской области. Полный текст технического задания можно увидеть в приложении к выпускной квалификационной работе. Также были предложены меры, которые позволят устранить недостатки, выявленные в ходе проведения анализа ИТ – инфраструктуры отделения Пенсионного Фонда России по Белгородской области.

3.2 Оценка экономической эффективности предлагаемых мероприятий по совершенствованию интегрированной системы охраны отделения Пенсионного Фонда России по белгородской области

При выполнении проекта по информатизации для любого предприятия вопрос об экономической эффективности выполняемых работ принципиально важен.

Проблема расчета экономической эффективности упирается в несколько моментов.

1) У заказчика есть понимание, что существующая в данный момент информационная система по некоторым критериям его не устраивает, он готов четко сформулировать эти критерии, но как только дело доходит до заключения договора с подрядчиком, данная четкость пропадает;

2) Заказчик хочет решить максимальное число проблем за минимальный промежуток времени, не обращая внимания на вопрос о том, что, сколько стоит и в какие сроки может быть реализовано;

3) Разработчик не видит по своей вине или по вине заказчика те ключевые моменты, которые принципиально важны для реализации проекта и которые оказывают прямое влияние на параметры экономических показателей системы.

Таким образом, для реализации каждого конкретного проекта модернизации или создания информационной системы необходимо четко определить, какие параметры и экономические показатели необходимо

ввести в экономическое обоснование, для того чтобы показать необходимость проектирования или внедрения, которое так же необходимо рассматривать как проект информационной системы.

В этом подпункте будет произведен расчет экономической эффективности проекта по модернизации интегрированной системы охраны отделения Пенсионного Фонда России по Белгородской области.

Первым делом посчитаем стоимость разработки проекта совершенствования интегрированной системы охраны. Сюда можно включить:

— Затраты на научно – исследовательскую работу: затраты на теоретические исследования предметной области, составление и утверждение технического задания на модернизацию системы (КНИР);

— Затраты на анализ существующей системы безопасности, ее совершенствование;

— затраты на приобретение перечня необходимого оборудования, его установку, подбор и обучение персонала работе с новой версией продукта (КНОВ);

— общие капитальные вложения, включая затраты на НИР и новое оборудование.

В смету затрат на научно – исследовательскую работу включаются:

— материальные затраты;

— амортизационные отчисления;

— затраты на эксплуатацию оборудования;

— затраты на программное обеспечение при использовании ЭВМ;

В таблице 3.3 представлен график научно – исследовательской работы и ее трудоемкость.

Процент трудоемкости действий произведем методом пропорции:

147 дней – 100%

14 дней - 14·100/147 =9.52 %;

21 день - 21·100/147 =14.28 %;

60 дней - 60·100/147 =40.82 %;

14 дней - 14·100/147 =9.52 %;

31 день - 31·100/147 =21.09 %;

7 дней - 7·100/147 =4.76 %.

Таблица 3.3 – Оценка трудоемкости выполнения дипломного проекта

Виды выполненных работ	Трудоемкость	
	дней	%
Разработка технического задания. Изучение сопутствующей литературы	14	6,82
Изучение предметной области и постановка задачи	21	9,09
Анализ деятельности рассматриваемой организации. Построение графиков, диаграмм, разработка рекомендаций по модернизации существующей информационной системы, проведение необходимых работ по модернизации	60	59,09
Выводы о проделанной работе	14	9,09
Подготовка отчетной документации	31	13,64
Защита отчета, утверждение результатов	7	2,27
Итого:	147	100

Далее, рассчитаем материальные затраты на выполнение научно – исследовательской работы. Все затраты в актуальных ценах представлены в таблице 3.4

Таблица 3.4 – Смета затрат на приобретение покупных комплектующих изделий разработчиком

Наименование изделия	Тип	Количество, шт.	Стоимость за ед., руб.	Стоимость, руб.
Упаковка бумаги	«Снегурочка», 90 г/м^{2,} формат А4, 500л	1	210	210
Заправка картриджа принтера	Canon LBP 2900B	1	300	300
Шариковая ручка	Brauberg	4	25	100
Блокнот, 96л	Brauberg	1	70	70
Линейка, 30 см	Brauberg	1	32	32
Скрепки	Brauberg, 28 мм, 100 шт.	1	45	45
Итого:				757

Амортизация использованных в период выполнения научно – исследовательской работы оборудования, инструментов и ЭВМ рассчитывается по формуле:

$$A_м = \frac{O_ф \cdot H_а \cdot T_м}{365 \cdot 100} \ , \qquad (3.1)$$

где $О_ф$ – стоимость используемого оборудования;

$Н_а$ – норма амортизации, %;

$Т_м$ – время эксплуатации оборудования за период проведения научно – исследовательской работы, дни.

Для определения общей суммы амортизационных отчислений по всему используемому и оборудованию составлена смета (таблица 3.5).

Таблица 3.5 – Смета амортизационных отчислений за период научно – исследовательской работы

Вид оборудования	Стоимость, руб.	Время пользования, дней	Годовая норма амортизации, %	Сумма амортизации за период НИР, руб.
Ноутбук HP Probook 440 G3	45000	147	20	3624,6
Принтер Canon LBP 2900B	4500	20	20	49,3
Сетевой фильтр SVEN	1000	147	20	80.5
Мышь Lenovo	600	147	20	48,3
Итого:	51100			3758,7

Затраты на эксплуатацию оборудования (Ноутбук и принтер) включают стоимость электроэнергии (таблица 3.2.4):

$$З_{эл} = С_{эл} \cdot М_м \cdot Т_м \cdot Т_{сут} \ , \qquad (3.2)$$

где $С_{эл}$ – стоимость 1 кВт/ч электроэнергии, руб.;

$М_м$ – мощность оборудования, кВт/ч;

$T_м$ - время эксплуатации оборудования за период научно – исследовательской работы;

$T_{сут}$ – время работы оборудования в сутки.

Таблица 3.6 – Параметры эксплуатации оборудования за период научно – исследовательской работы

Параметр	Значение
Стоимость 1 кВт/ч электроэнергии	3,53 руб.
Мощность ноутбука	0,5 кВт/ч
Мощность принтера	0,1 кВт/ч
Время эксплуатации ноутбука за период НИР	147 дней
Время эксплуатации принтера за период НИР	20 дней
Время работы ноутбука в сутки	6 часов
Время работы принтера в сутки	0,1 часа

Затраты на эксплуатацию оборудования составляют:

$З_{эл} = (3,53 \cdot 0,5 \cdot 147 \cdot 6) + (3,53 \cdot 0,1 \cdot 20 \cdot 0,1) = 1557,43$ руб.

Затраты на программное обеспечение при использовании компьютера включают стоимость программных продуктов на период выполнения научно – исследовательской работы (таблица 3.7).

Таблица 3.7 – Смета затрат на программное обеспечение

Программное обеспечение	Марка, тип	Количество, шт.	Цена за единицу, руб.	Стоимость, руб.
Windows 10	USB	1	7900	7900
Office 2016	DVD	1	3990	3990
Aris Express	Installer	1	Бесплатно	0
Итого:				11890

По данным предыдущих расчетов составлена смета затрат на выполнение научно – исследовательской работы (таблица 3.8).

Таблица 3.8 – Смета затрат на выполнение НИР

Наименование затрат	Сумма, руб.
Материальные затраты	757
Основная зарплата разработчиков	3758,7
Амортизационные отчисления	2305,03
Затраты на эксплуатацию оборудования	1557,43
Затраты на программное обеспечение	11890
Итого: $К_{нир}$	20268,16

Совершенствование интегрированной системы охраны потребует затрат на приобретение нового аппаратного и программного обеспечения (Кнов):

$$К_{нов} = К_{пр} + К_{мон}, \quad (3.3)$$

$К_{пр}$ – прейскурантная стоимость закупаемого оборудования;

$К_{мон}$ – затраты на транспортировку и монтаж оборудования, равные 5 % от прейскурантной стоимости.

В таблице 3.9 приведена прейскурантная стоимость закупаемого оборудования и программного обеспечения, необходимого для работы интегрированной системы охраны.

Затраты на транспортировку и монтаж оборудования составляют:

$К_{мон} = 2368902 \cdot 0,05 = 118445,1$ руб.

Капитальные затраты на приобретение оборудования и программного обеспечения (Кнов) составляют:

$К_{нов} = 2368902 + 118445,1 = 2487347,1$ руб.

Таким образом, общие капитальные вложения на модернизацию информационной системы определяются по формуле:

$$К_{общ} = К_{нир} + К_{нов}, \quad (3.4)$$

где $К_{общ}$ – общие капитальные вложения.

$К_{общ} = 20268,16 + 2487347,1 = 2507615,26$ руб.

Таблица 3.9 – Прейскурантная стоимость закупаемого оборудования и ПО

Наименование покупных изделий	Марка, тип	Кол-во, шт.	Цена за ед., руб.	Стоимость, руб.
Персональный компьютер в сборе, необходимый для работы интегрированной системы охраны	Сборка	1	60000	60000
Жесткий диск для RAID массива	Seagate 5900 SkyHawk 2 Тб	1	5199	5199
Коммутатор сетевой	hp 1810-24	2	9524	18508
Программное обеспечение	ПО Администратор базы данных Орион Про	1	4 719	4 719
Программное обеспечение	ПО Генератор отчетов Орион Про	1	2160	2160
Программное обеспечение	ПО Учет рабочего времени Орион Про	1	4719	4719
Программное обеспечение	Оперативная задача "ОЗ Орион Про" исп.4, шт.	1	9439	9439
Программное обеспечение	ПО "Монитор Орион Про"	1	4719	4719
Программное обеспечение	ПО Центральный сервер Орион Про	1	9439	9439
Сборка персонального компьютера	Сборка	50	45000	2250000
Итого: $К_{пр}$				2368902

После проведения работ по модернизации интегрированной системы охраны отделения Пенсионного Фонда России по Белгородской области можно заметить, что время выполнения действий в случае возникновения чрезвычайной ситуации существенно сократилось. Причиной тому стала закладка в программную часть уже продуманной последовательности действий, которые система выполняет сама, без участия человека. Новая интегрированная система охраны позволяет значительно быстрее реагировать на возможные чрезвычайные ситуации. Также система охраны стала более самостоятельной, и теперь для контроля ее работы необходим всего 1 сотрудник с базовыми навыками пользователя ПК, что также

позволяет сократить число сотрудников, которые работают с системой. Расчеты сокращения времени представлены в таблице 3.10

Таблица 3.10 – таблица расчетов сокращения времени на выполнение различных операций

Действие	Время до внедрения,	Время после внедрения,	Сэкономленное время
Подтверждение возгорания	5 мин.	1 мин.	4 мин.
Неавторизованный доступ	5 мин	30 сек	4 мин 30 сек
Проникновение на охраняемый объект	от 5 мин. и выше	15 сек	минимум 4 мин 45 сек
Эвакуация персонала	10 мин	3 мин	7 мин
Ежедневное время, которое необходимо уделять на мониторинг безопасности	6 часов	1 час	5 часов

Также, так как был заменен ряд морально устаревшего оборудования, существенно возросла производительность труда. Замена локальной сети обеспечила стабильность работы последней. Установка недостающих источников бесперебойного питания на абсолютно всех компьютерах организации ликвидировала зависимость организации от постоянной подачи тока и минимизировала потерю важных данных.

Новые персональные компьютеры позволили существенно сократить выполнение сотрудниками различных рабочих процессов. До обновления парка компьютеров, некоторые машины запускали необходимые программы вплоть до 10 секунд. Теперь же скорость запуска приложений сократилась до 1-2 секунд. Новое аппаратное обеспечение также позволило устанавливать более удобное, современное и высокопроизводительное программное обеспечение.

Оценивая эффективность от модернизации интегрированной системы организации сложно говорить о каких-либо экономических показателях, ведь продукт предназначен для внутреннего пользования, а не для извлечения прибыли. Также, рассматриваемая организация не является коммерческой. Ожидаемую прибыль вычислить не получится, потому что модернизация

системы не влияет на доход организации, а только автоматизирует деятельность сотрудника службы безопасности и высвобождает ему время, которое может быть использовано для выполнения других должностных обязанностей.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы были выявлены и проанализированы требования, предъявляемые к информационной системе. После детального изучения деятельности отделения Пенсионного Фонда России по Белгородской области, было разработано техническое задание на модернизацию интегрированной системы охраны. Для реализации данной идеи не потребовалось какое – либо специальное программное обеспечение.

Исходя из выявленных требований, интегрированная система охраны в отделении Пенсионного Фонда России по Белгородской области будет модернизирована. Улучшение позволит автоматизировать процесс контроля за безопасностью на подконтрольном объекте, а также сократить время реакции на различные явления, что при возникновении реальной чрезвычайной ситуации поможет спасти здоровье и жизни сотрудников, а также важную рабочую документацию.

Все работы проведены с учетом всех особенностей деятельности отделения Пенсионного Фонда России по Белгородской области. Для работы с автоматизированным рабочим местом интегрированной системы охраны сотруднику требуются только базовые навыки работы с персональным компьютером. Никаких специальных знаний не требуется.

Реализованный проект охватывает все потоки информации, имеющиеся в данном отделении Пенсионного Фонда, и позволяет автоматизировать работу сотрудника службы безопасности. Предложенные в данной выпускной квалификационной работе рекомендации обязательно будут использованы при модернизации интегрированной системы охраны, которое запланировано на июль этого года.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Studwood – учебные материалы онлайн [Электронный ресурс]. – Режим доступа: https://studwood.ru/733359/ekonomika/teoreticheskie_aspekty_obespecheniya_bezopasnosti_predpriyatiya (дата обращения 30.05.2018г).
2. Словари и энциклопедии на Академике [Электронный ресурс]. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/8410 (дата обращения 30.05.2018г).
3. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Пожарная_безопасность (дата обращения 30.05.2018г).
4. Fb.ru [Электронный ресурс]. – Режим доступа: http://fb.ru/article/255232/integrirovannyie-sistemyi-bezopasnosti-klassifikatsiya-proektirovanie-oborudovanie (дата обращения 30.05.2018г).
5. Secuteck – технологии безопасности [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/articles2/pronsol/klassifikaciya_integrirovannih_sisitem_bexopasnocti_page34 (дата обращения 30.05.2018г).
6. Системы безопасности Болид [Электронный ресурс]. – Режим доступа: https://bolid.ru/production/orion/po-orion/po-arm/arm_orion_pro.html#descr (дата обращения 30.05.2018г).
7. Syl.ru – метод фокус – группы [Электронный ресурс]. – Режим доступа: https://www.syl.ru/article/201467/new_fokus-gruppa---eto-chto-takoe-metod-fokus-gruppyi (дата обращения 30.05.2018г).
8. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/SWOT-анализ (дата обращения 30.05.2018г).

9. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Техническое_задание (дата обращения 30.05.2018г).

10. Fb.ru [Электронный ресурс]. – Режим доступа: http://fb.ru/article/258324/tehnicheskoe-zadanie---eto-chto-takoe-ponyatie-i-soderjanie-kak-sostavit-tz (дата обращения 30.05.2018г).

11. Сайт компании ООО «Системы Комплексной безопасности» [Электронный ресурс]. – Режим доступа: http://skb-security.ru/about (дата обращения 30.05.2018г).

12. Сайт компании ООО «Белгородская Монтажная Компания» [Электронный ресурс]. – Режим доступа: http://bmk-31.ru/ (дата обращения 30.05.2018г).

13. Сайт компании «Системы безопасности КОДОС» [Электронный ресурс]. – Режим доступа: http://kodos.ru/ (дата обращения 30.05.2018г).

14. Сайт компании «Системы безопасности Болид» [Электронный ресурс]. – Режим доступа: https://bolid.ru/ (дата обращения 30.05.2018г).

15. ИТ аутсорсинг и консалтинг [Электронный ресурс]. – Режим доступа: https://helpit.me/articles/analiz-it-i-informacionnoi-infrastruktury (дата обращения 30.05.2018г).

16. Стек – ИТ аутсорсинг [Электронный ресурс]. – Режим доступа: https://www.stekspb.ru/autsorsing-it-infrastruktury/it-glossary/it-analysis/ (дата обращения 30.05.2018г).

17. Refleader.ru [Электронный ресурс]/Электрон. дан. – Режим доступа: https://refleader.ru/otryfsabew.html (дата обращения 30.05.2018г).

18. BLOGSISADMINA.RU [Электронный ресурс]/Электрон. дан. – Режим доступа: http://blogsisadmina.ru/seti/topologii-setej.html (дата обращения 30.05.2018г).

19. SOFTHOLM.COM [Электронный ресурс]/Электрон. дан. – Режим доступа: http://www.softholm.com/news/computers/article_2451.html, (дата обращения 30.05.2018г).

20. Book.kbsu.ru [Электронный ресурс]/Электрон. дан. – Режим доступа: https://book.kbsu.ru/theory/chapter6/1_6.html (дата обращения 30.05.2018г).

21. INTERFACE.RU [Электронный ресурс]/Электрон. дан. – Режим доступа: https://interface.ru/home.asp?artId=106 (дата обращения 30.05.2018г).

22. ГОСТ 34.602-89 - Информационная технология. Комплекс стандартов на автоматизированные системы.

23. Алиев, В.С. Информационные технологии и системы финансового менеджмента [Текст]/— Санкт-Петербург, Инфра-М, 2007 г.- 320 с.

24. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью[Текст]/ Сенаторов М. Ю., Толстой А. И. — Санкт-Петербург, Горячая Линия - Телеком, 2014 г.- 216 с.

25. Казакова, Н.А. Финансовый анализ. Учебник и практикум[Текст]/— Москва, Юрайт, 2015 г.- 544 с.

26. Информационные системы и технологии: Научное издание[Текст]/ Под ред. Ю.Ф. Тельнова. - М.: ЮНИТИ, 2016. - 303 с.

27. ГОСТ 24.701-86 «Надежность автоматизированных систем управления».

28. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания.

29. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие [Текст]/ А.В. Васильков, А.А. Васильков, И.А. Васильков. - Москва: Форум, 2013. - 528 с.

30. Гукова, А.В. Управление предприятием: финансовые и инвестиционные решения: Курс лекций для бакалавров: Учебное пособие [Текст]/ А.В. Гукова, И.Д. Аникина, Р.С. Беков. - Москва: ФиС, ИНФРА, 2012. - 184 с.

31. Кравченко, Л.И. Анализ хозяйственной деятельности в торговле: учебник[Текст]/Л.И. Кравченко. – Москва: новое знание, 2014. – 544 с.

32. Pro – spo.ru – свободное программное обеспечение и новые информационные технологии [Электронный ресурс] – Режим доступа: http://pro-spo.ru/bisness-processing/2662--allfusion-process-modeler, свободный (дата обращения 30.05.2018г).

33. Корпоративный менеджмент: финансы, бизнес – планы, управление компанией [Электронный ресурс] – Режим доступа: http://www.cfin.ru/vernikov/idef/idef3.shtml, свободный (дата обращения 30.05.2018г).

34. StudFiles – файловый архив для студентов [Электронный ресурс] – Режим доступа: http://www.studfiles.ru/preview/5943741/page:10/, свободный (дата обращения 30.05.2018г).

35. Персональный сайт Иванова А.М [Электронный ресурс]/Электрон. дан. – Режим доступа: http://иванов-ам.рф/informatika_10/informatika_materialy_zanytii_10_60.html, свободный (дата обращения 30.05.2018г).

36. Виханский О.С. Стратегическое управление[Текст]/ - М.: Издательство Московского Университета, 2007. -164 с.

37. Грекул, В.И. Проектирование информационных систем : учеб. пособие. / В.И. Грекул, Н.Л. Коровкина, Ю.В. Куприянов – М. : Национальный Открытый Университет «ИНТУИТ», 2012. – 187 с.

38. Раскин, Д. Интерфейс: новые направления в проектировании компью- терных систем : [пер. с англ.] / Д. Раскин. – СПб. : Символ-Плюс, 2000. – 272 с.

39. Мазур И.И. Реструктуризация предприятий и компаний: Учеб. пособие для вузов/И.И Мазур, В.Д Шапиро- М.: ЗАО "Издательство "Экономика", 2014.

40. Мацяшек, Л. Анализ и проектирование информационных систем : [пер. с англ.] / Л. Мацяшек. – М. : И. Д. Вильямс, 2008. – 814 с.

ПРИЛОЖЕНИЕ

УТВЕРЖДАЮ
Начальник отдела
по защите информации
ОПФР по Белгородской
области

_____Ушаков А.П.

«___» _____ 2018г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по модернизации интегрированной системы охраны и управления доступом административного здания Государственного учреждения - Отделения Пенсионного Фонда Российской Федерации по Белгородской области

г. Белгород

Настоящим техническим заданием предусмотрено выполнение работ по модернизации системы контроля и управления доступом (далее - СКУД), используя технические средства (материалы, изделия и конструкции, приобретаемые за счет Исполнителя государственного контракта) указанные в Приложении 1 к техническому заданию.

1. Общие сведения

1.1 Наименование системы

Полное наименование: Интегрированная Система Охраны Отделения Пенсионного Фонда России по Белгородской области

Краткое наименование: ИСО «ОПФР по Белгородской области».

1.2 Основания для выполнения работ

Работы выполняется на основании Государственного контракта, заключенного с Исполнителем по результатам проведения электронного аукциона на сайте единой информационной системе в сфере закупок (http://zakupki.gov.ru)

1.3 Наименование организаций – Заказчика и Разработчиков

Заказчик: ОПФР по Белгородской области

Адрес фактический: г. Белгород, ул. Преображенская, строение №87

Телефон/Факс: +7 (4722) 30-69-67

Разработчик: студент 4 курса очного отделения группы 07001422, Тутов Иван Михайлович

Адрес фактический: г. Белгород, ул. Дегтярева, д.2, кв.104.

Телефон/Факс: +79524351996

1.4 Плановые сроки начала и окончания работы

Начало работ – 10.07.2019г

Окончание работ – 25.08.2019г

1.5 Источники и порядок финансирования

Все необходимые для проекта технические средства (материалы, изделия и конструкции) приобретаются за счет Исполнителя государственного контракта.

1.6 Порядок оформления и предъявления заказчику результатов работ

Работы по модернизации ИСО ОПФР по Белгородской области сдаются Разработчиком поэтапно в соответствии с календарным планом Проекта. По окончании каждого из этапов работ Разработчик сдает Заказчику соответствующие отчетные документы этапа, состав которых определен Договором.

2. Назначение и цели создания системы

2.1 Назначение системы

Основным назначением ИСО ОПФР по Белгородской области является автоматизация работы сотрудников службы безопасности организации. В рамках проекта автоматизируется деятельность предприятия в следующих процессах:

1) разграничение и контроль доступа;
2) обеспечение физической безопасности на предприятии;
3) обеспечение противопожарной безопасности;
4) обеспечение защиты конфиденциальной информации, имеющейся в организации;
5) контроль периметра организации;
6) Составление итоговых отчетов о работе системы.

2.2 Цели модернизации системы

ИСО ОПФР по Белгородской области модернизируется с целью:

- повышения качества выполняемых системой функций;

- сокращения времени на выполнение заложенных в систему сценариев;
- упрощения работы для службы безопасности.

3. Характеристика объектов автоматизации

Государственное учреждение – Отделение Пенсионного Фонда России по Белгородской области является территориальным Пенсионного Фонда Российской Федерации. Отделение входит в единую централизованную систему органов управления средствами обязательного пенсионного страхования в Российской Федерации и в своей деятельности подотчетно Государственному учреждению – Пенсионному Фонду Российской Федерации.

Отделение осуществляет свою деятельность на территории Белгородской области во взаимодействии с органами государственной власти, органами местного самоуправления, многофункциональными центрами предоставления государственных и муниципальных услуг, организациями независимо от правовых форм и форм собственности, в том числе общественными организациями, а также физическими лицами.

Отделение осуществляет организацию деятельности подведомственных территориальных органов ПФР (далее – подведомственные территориальные органы), в том числе по вопросам:

- приема, проверки, оценки, обработки и учета документов в целях установления различных социальных выплат;
- принятия решений об установлении\отказе в установлении пенсий, пособий и иных социальных выплат, приостановления, прекращения, возобновления их выплат;
- начисления в лицевых счетах получателей сумм пенсий, пособий и иных социальных выплат;
- проведения перерасчета пенсий, пособий и иных социальных выплат;

- выплаты пенсий, пособий и иных социальных выплат;
- информирования застрахованных лиц о состоянии индивидуальных счетов и т.д.

Основные процессы, подлежащие модернизации приведены в таблице 1.1.

Таблица 1.1 – Основные процессы

Наименование процесса	**Возможность автоматизации**	**Решение об автоматизации в ходе проекта**
Контроль и управление доступом	Возможна	Будет модернизирован
Физическая безопасность на объекте	Возможна	Будет модернизирован
Пожарная безопасность	Возможна	Будет модернизирован
Защита конфиденциальной информации	Возможна	Будет модернизирован
Охрана периметра объекта	Возможна	Будет модернизирован
Учет рабочего времени	Возможна	Будет модернизирован

4. Требования к системе

4.1 Система контроля и управления доступом (СКУД).

4.1.1 Система контроля и управления доступом должна обеспечивать санкционированный доступ должностных лиц в помещения административного здания ОПФР по Белгородской области, препятствовать

несанкционированному проникновению или попыткам проникновения на охраняемый объект посторонних лиц, а также:

- идентификацию персонала и управление доступом в помещения;
- учет рабочего времени должностных лиц.

4.1.2. Холл ОПФР по Белгородской области должен быть оборудован турникетом с бесконтактным дистанционным считывателем, а также полуростовыми ограждениями зоны ожидания с калиткой для проезда инвалидных колясок (Приложение 2);

4.1.3. Каждый контролируемый проход должен быть оборудован бесконтактными дистанционными считывателями, замковыми устройствами.

4.1.4. Размещение системы должно отвечать требованиям:

- аппаратура, входящая в состав СКУД, должна быть выполнена в блочном исполнении;
- считыватели устанавливаются в коридорах здания.

4.1.5. Средствами системы контроля и разграничения доступа оборудуются 5 помещений (архивы – 3 шт., серверная, помещение Удостоверяющего Центра), где должно быть исключено несанкционированное пребывание посторонних лиц. Помещения должны быть постоянно закрытыми и запертыми.

4.1.6. Открывание замка для входа в указанные помещения обеспечивается дистанционными считывателями смарт-карт. Отпирание замка для выхода из помещения осуществляется нажатием специальной кнопки.

4.2. Электропитание.

4.2.1. Обеспечение электроснабжением СКУД должно соответствовать требованиям СНиП 2.04.09-84 и РД 78.143-92.

4.2.2. Электропитание комплексной системы безопасности должно обеспечиваться по первой категории.

4.2.3. Система бесперебойного питания должна обеспечивать надежную работу системы при:

- длительном пропадании напряжения питающей сети;
- кратковременном падении (провале) напряжения питающей сети;
- импульсных и кратковременных перенапряжениях.

4.2.4. Система бесперебойного питания строится по распределённой схеме и должна обеспечить выполнение следующих функций:

- автономное электропитание оборудования СКУД при отсутствии напряжения в сети переменного тока;
- защиту активного сетевого оборудования от импульсных помех внешней электросети и от перенапряжения;
- поддержание максимальной ёмкости аккумуляторных батарей при наличии сети переменного тока;
- защиту аккумуляторных батарей от перезарядки и глубокого разряда;
- защиту стабилизатора от коротких замыканий по выходу;
- поддержку номинальных значений электропитания устройств СКУД независимо от наличия основного источника электропитания - сети переменного тока 220 В 50 Гц.

4.2.5. Устанавливаемые на объекте ИБП должны отвечать требованиям ГОСТ 27699-88 и ГОСТ Р 50745-95 и:

- работать в широком диапазоне изменения входного напряжения (не менее+15%);
- иметь значение коэффициента входной мощности близкое к единице;
- коэффициент гармонических искажений на входе не более 8%;
- иметь высокую перегрузочную способность (не менее 200% в течение 1 минуты и 125% в течение 10 минут) и устойчивость к большим фазовым перекосам;

- иметь КПД не ниже 92-94%;
- при переходе на питание от аккумуляторных батарей, переключаться без разрыва синусоиды, т.е. работать в режиме ON-LINE;
- иметь высококачественные герметичные необслуживаемые аккумуляторные батареи со сроком службы 10-15 лет;
- иметь удобную и гибкую систему управления.

4.2.6. Источники бесперебойного питания должны обеспечивать работу СКУД в «дежурном режиме» не менее 4 часов, а в режиме «Тревога» – не менее 1 часа.

4.2.7. Электроснабжение подсистем КСБ должно осуществляться от свободных групп щита дежурного освещения в электрощитовой.

4.2.8. Электропитание комплекса СКУД осуществляется от сети переменного тока напряжением 220+10 % В от отдельного электрощита.

4.2.9. Обеспечение аварийного электропитание СКУД от источника бесперебойного питания.

4.3. Электрические проводки.

4.3.1. Электрические проводки должны подразделяться на:

- линии связи (шлейфы сигнализации, цепи управления, шины данных, интерфейсные шины);
- низковольтные цепи питания (12/24 В постоянного тока);
- высоковольтные цепи питания (220/380 В переменного тока частотой 50 Гц).

4.3.2. Проектирование линий связи и низковольтных цепей питания должно осуществляться с учетом требований ПУЭ, СНиП 3.05.06-85. Выбор кабелей и проводов производить с учетом их технических характеристик. Прокладка данных цепей должна производиться: скрыто в штробе; в лотках за подвесными потолками, в трубах ПВХ, в электротехническом коробе.

4.3.3. Проектирование высоковольтных цепей питания должно осуществляться в металлических трубах. В местах прохождения проводов и кабелей через стены или перекрытия должны быть предусмотрены огнестойкие уплотнения

4.4. Заземление.

4.4.1. Защитное заземление или заземление технических средств должно соответствовать ПУЭ, СНиП 3.05.06-85, ГОСТ 12.1.030-81 и технической документации на аппаратуру СКУД.

4.5. Требования к численности и квалификации персонала

4.5.1. Для обеспечения эксплуатация интегрированной системы охраны необходимо выделить одного работника, который будет работать с АРМ системы.

4.5.2. К квалификации персонала, эксплуатирующего ИСО ОПФР по Белгородской области, предъявляются следующие требования:

- конечный пользователь - знание соответствующей предметной области, знания и навыки работы с приложениями операционной системы Windows;

- системный администратор - знание методологии проектирования баз данных, знание СУБД, знание языка запросов SQL.

4.5.3. система реализуется на персональном компьютере, и требования к организации труда сотрудника и режимах отдыха при работе с системой должны устанавливаться с учетом этого типа вычислительной техники.

4.6. Требования к информационной безопасности

4.6.1. Защита системы должны быть обеспечена аппаратно – программным комплексом защитных средств.

4.6.2. система должна находиться под защитой во всех режимах ее функционирования и на всех технологических этапах обработки информации.

4.6.3. программные комплексы не должны каким – либо образом замедлять быстродействие системы.

4.6.4. на компьютере – АРМ необходимо наличие средств антивирусной защиты актуальной версии.

4.6.5. система должна поддерживать возможность создания резервных копий.

5. Состав и содержание работ по созданию системы

5.1 Работы по созданию системы выполняются в три этапа:

1) Проектирование. Разработка эскизного проекта. Разработка технического проекта.
2) Разработка рабочей документации. Адаптация программ.
3) Ввод в действие.

Конкретные сроки выполнения стадий и этапов разработки и создания Системы определяются Планом выполнения работ, являющимся неотъемлемой частью Договора на выполнение работ по настоящему техническому заданию.

6. Порядок контроля и приёмки системы

6.1. Система подвергается испытаниям следующих видов:

1. Предварительные испытания.
2. Опытная эксплуатация.
3. Приемочные испытания.

6.2. Состав, объем и методы предварительных испытаний системы определяются документом «Программа и методика испытаний», разрабатываемым на стадии «Рабочая документация».

6.3. Состав, объем и методы опытной эксплуатации системы определяются документом «Программа опытной эксплуатации», разрабатываемым на стадии «Ввод в действие».

6.4. Состав, объем и методы приемочных испытаний системы определяются документом «Программа и методика испытаний», разрабатываемым на стадии «Ввод в действие» с учетом результатов проведения предварительных испытаний и опытной эксплуатации.

Ведущий специалист-эксперт

отдела по защите информации А.И.Жуковский

Приложение №1

к техническому заданию

№ п.п.	Наименование работ и затрат, материалов, изделий и конструкций	Ед. изм.	Кол-во
1	2	3	4
Монтажные работы			
1.	Настройка простых сетевых трактов: конфигурация и настройка сетевых компонентов (мост, маршрутизатор, модем и т.п.) (п. 26; 31)	1 шт.	2
2.	Настройка простых сетевых трактов: программирование сетевого элемента и отладка его работы (мультиплексор, регенератор) (п. 25; 27; 28)	1 сетевой элемент	1
3.	Приборы приемно-контрольные объектовые на: 1 луч (п. 32)	1 шт.	1
4.	Устройства промежуточные на количество лучей: 1 (п. 33)	1 шт.	5
5.	Приборы ПС на: 4 луча (п. 34)	1 шт.	1
6.	Извещатель ОС автоматический: контактный, магнитоконтактный на открывание окон, дверей (п. 36)	1 шт.	4
7.	Отдельно устанавливаемый: преобразователь или блок питания (п. 30; 50; 51)	1 шт.	7
8.	Стойка фиксаторная (п. 42; 43; 44; 45)	1 шт.	8
9.	Устройство ультразвуковое,: преобразователь (излучатель или приемник) (п. 35)	1 шт.	1
10.	Механизм исполнительный, масса: до 50 кг (п. 41; 48)	1 шт.	4
11.	Механизм исполнительный, масса: до 100 кг (п. 40)	1 шт.	1
12.	Провод двух- и трехжильный с разделительным основанием по стенам и потолкам, прокладываемый по основаниям: бетонным и металлическим (п. 59)	100 м	1

13.	Аппарат настенный, масса от 0,15 т до 0,2 т (п.29)	1 шт.	1
14.	Измерение сопротивления шлейфа, сопротивления изоляции и омической асимметрии	1 усил. участок цепи	12
15.	Устройство сигнально-блокировочное (п. 38)	1 шт.	11
16.	Аппарат (кнопка, ключ управления, замок электромагнитной блокировки, звуковой сигнал, сигнальная лампа) управления и сигнализации, количество подключаемых концов: до 2 (п. 37)	1 шт.	4
17.	Автомат одно-, двух-, трехполюсный, устанавливаемый на конструкции: на стене или колонне, на ток до 25 А (п. 52)	1 шт.	6
18.	Аккумулятор кислотный стационарный, тип: С-1, СК-1 (п. 53)	1 шт.	6
19.	Труба винипластовая по установленным конструкциям, по стенам и колоннам с креплением скобами, диаметр: до 25 мм (п. 60)	100 м	1
20.	Затягивание провода в проложенные трубы и металлические рукава первого одножильного или многожильного в общей оплетке, суммарное сечение: до 2,5 мм2	100 м	1
21.	Короб металлический по стенам и потолкам, длина: 2 м (п. 61; 62)	100 м	1
22.	Провод в коробах, сечением: до 6 мм2	100 м	1,8
Пусконаладочные работы			
23.	Автоматизированная система управления II категории технической сложности с количеством каналов (Кобщ): 10	1 система	1
24.	Автоматизированная система управления II категории технической сложности с количеством каналов (Кобщ): за каждый канал свыше 10 до 19 добавлять к расценке 02-01-002-03	1 канал	2
Оборудование и материалы			
25.	Системный блок (процессор двухядерный 2,8 Ггц, жесткий диск 500Gb, DVD- привод,форм-фактор	шт.	1

	mATX, мощность 600Вт		
26.	Microsoft Windows 10 Enterprise 64-bit Рус (OEM), Операционная система	шт.	1
27.	Клавиатура USB	шт.	1
28.	Лазерный манипулятор "мышь", USB	шт.	1
	LG Flatron L1742SE-BF, 21" TFT монитор (или эквивалент) Тип матрицы : TFT TN Размер экрана (дюйм) : 21 Разрешение дисплея (pix) : 1920x1080 Яркость (кд/м2) : 250 Динамическая контрастность : 8000:1 Время отклика (мс) : 5 Угол обзора (горизонтальный) : 160 Угол обзора (вертикальный) : 160 Разъем VGA : 1 Высота (мм) : 389 Ширина (мм) : 469 Толщина (мм) : 184	шт.	1
29.	Источник бесперебойного питания 1000ВА (600Вт)	шт.	1
30.	АРМ Орион ПРО, программное обеспечение и ключ защиты на 10 устройства (или эквивалент) **Функциональные возможности** **Сервер "Орион Про"** • взаимодействие с базой данных (MS SQL Server 2005/ 2008/2012), передача данных по сети на рабочие места **Оперативная задача** • Графическое отображение состояний зон, разделов, точек доступа, приемно-контрольных приборов системы, считывающих устройств, видеокамер на планах помещений	комплект	1

	• Управление взятием и снятием разделов и зон, как из АРМ, так и удаленно - со считывателей приборов («С2000-2», «С2000-4», «Сигнал-20П», «С2000-КДЛ») и с клавиатур («С2000-К», «С2000-КС»), а так же выдача специализированных команд точкам доступа, считывающим устройствам, видеокамерам • Речевое оповещение по тревогам, возможность записи и воспроизведения пользовательских сообщений • Протоколирование всех событий, происходящих в системе • Организация распределенной системы контроля доступа в ИСО «Орион» • Механизм разграничения полномочий по доступу и управлению объектами для персонала и посетителей • Гибкое разграничение полномочий операторов за счет многоуровневой системы паролей • Поддержка сценариев управления, позволяющих выдавать одну или комплекс команд приемно-контрольным приборам, исполнительным устройствам, а также программному обеспечению системы, как по событию в системе или временному расписанию, так и по команде оператора • Графическое отображение статистики АЦП и сопротивления шлейфов сигнализации, уровня задымленности (запыленности) адресно-аналоговых дымовых и температуры адресно-аналоговых тепловых датчиков • Вывод информационных карточек по каждому элементу системы, а также по персоналу или посетителям объекта • Трансляция текстовых сообщений с отображением на клавиатуре С2000-К или передаче пользователю с помощью С2000-ИТ • Защита системы от запуска несанкционированных программ • Интеграция видеосистем сторонних производителей: «Интеллект» (ITV), «Phobos» (Vocord), «Инспектор+» (ISS), «VideoNet» (Пентакон), «Trassir» (DSSL), «VideoSpider» (DarimVision), «CVS» (CVSNT), «GOAL» (СпецЛаб), «Macroscop» (Сателлит		

	Инновация), EWKLID. Благодаря интеграции пользователь может использовать данные видеосистемы совместно с Оперативной задачей АРМ «Орион» и организовать их взаимодействие посредством настройки логических связей. **Администратор базы данных "Орион Про"** • создание базы данных охраняемого объекта для ОПС, СКУД, пожаротушения и системы видеонаблюдения; • занесение планов охраняемых объектов в базу и размещение на них объектов охраны; • конфигурирование логических объектов охраны, таких как: зона, раздел, группа разделов, точка доступа, зона доступа; • формирование базы данных "Бюро пропусков": создание списка сотрудников с указанием для каждого человека всех необходимых атрибутов: личные данные, информации о принадлежности к подразделению и фирме. Возможность изменения названий полей в форме отображения данных сотрудника; • создание полномочий СКУД и ОПС, ограничение управления с помощью задаваемых администратором полномочий для выданных ключей и паролей; • прописывание полномочий доступа в контроллеры в режиме реального времени, а также обновление данных о СКУД на рабочих местах без общей перегрузки базы данных; • формирование базы данных "Учета рабочего времени": график работы, правила расчета графика работы для сотрудника и подразделений; • программирование сценариев управления с помощью шаблонов и специального встроенного языка программирования "Орион - Скрипт"; • настройка автоматической реакции системы на любые события; • возможность работы нескольких модулей "Администратор базы данных" в одной системе, механизм оповещения об обновлении данных при одновременном их		

	редактировании; • возможность печати карточки сотрудников на специализированном принтере. • настройка IP-камер, IP-видеосерверов и DVR • автоматическая регистрация информации документов удостоверяющих личность используя API для распознавания паспортов(необходимо приобрести SDK Cognitive Api) • возможность регистрации информации о посетителях, задания правил управления доступом • возможность помещать сотрудников в архив и восстанавливать их из архива • возможность автоматического оповещения по email для ответственных лиц, в виде карточки о посетителе после завершения регистрации • регистрация нарушителей **Монитор "Орион Про"** • отображение на интерактивных графических планах состояния охраняемого объекта, управление логическими объектами ОПС, системы пожаротушения, видеонаблюдения и СКУД; • регистрация и обработка возникающих в системе тревог - указание причины, служебных отметок, архивирование; • строгая привязка отображаемых и управляемых объектов системы безопасности к правам пароля, под которым дежурный офицер заступил на дежурство; • отображение протокола событий; • установка различных фильтров для отображения протокола событий; • возможность выборки событий в протоколе по заданным пользователем критериям; • предоставление дежурному офицеру информации (в виде карточки объекта) об объектах системы безопасности, таких как зона, прибор, раздел, группа разделов, дверь, зона доступа, видеокамера; • отображение информации СКУД - место нахождения сотрудника (с точностью до зоны доступа), нарушение трудовой дисциплины		

	при проходе через точку доступа; • осуществление запуска сценариев управления, как по "горячей" клавише, так и с помощью специальных элементов интерфейса (элементы дерева управления); • гибкая настройка интерфейса "Монитора системы" за счет реализации "плавающих" окон; • возможность предоставления "принудительного" доступа для сотрудников оператором системы. **Ядро системы (только в составе РМ Оперативная задача)** • опрос и управление приборами, подключенными по RS-485 к данному компьютеру, контроль видеокамер, подключенных к видеосистеме; • определение состояний контролируемых объектов системы (таких как зона, раздел, группа разделов, точка доступа и т.д.); • централизованное управление контролем доступа, взятием/снятием охраняемых зон, а также взятием/снятием разделов и групп разделов системы, запуск тактик управления реле; • отработка сценариев управления при возникновении соответствующего события; • взаимодействия с объектами всех сетевых рабочих мест системы (запуск сценариев управления, трансляция команд и т.д.); • прописывания полномочий СКУД в контроллеры доступа. **Генератор отчетов "Орион Про"** • формирование и выдача отчетов по различным категориям событий системы, таким как охранно-пожарные события, события доступа, вспомогательные отчеты о конфигурации системы; • формирование отчетов о полномочиях сотрудников, о конфигурации СКУД (для каждой точки доступа формируется список сотрудников, которые могут проходить через нее), о сотрудниках системы (какой фирме и		

	подразделению принадлежат, статус сотрудника и т.д.); • возможность настройки фильтров по времени, категориям событий, элементам системы безопасности; • возможность экспорта в MS Office (Word, Excel), Open Office (Writer, Calc), HTML PDF; • возможность построения отчетов через Internet; • возможность построения пользователем собственного отчета с помощью разработанного архитектора отчетов. **Учет рабочего времени "Орион Про"** • учет рабочего времени сотрудников охраняемого объекта, анализ и контроль соблюдения трудовой дисциплины на данном объекте; • поддержка как линейных (недельных) графиков работы, так и сменных; • экспорт отчетов и данных, необходимых для реализации собственного учета рабочего времени клиентами (при использовании компоненты интеграции с 1С Предприятие 8) с помощью специальной компоненты. **Персональная карточка** • Сетевой модуль • Поддерживает прямое соединение ПК сервера и клиента и через протокол TCP/IP • Позволяет провести фотоверификацию сотрудника или посетителя, транслируя в программу-клиент информационную карточку в автоматическом режиме по событию в системе контроля доступа **Видеосервер** • модуль, предназначенный для взаимодействия с сетевыми ip-камерами и система видеонаблюдения **Редактор планов помещений** — утилита для быстрой прорисовки планов объекта с использованием библиотеки графических элементов **Проверка шлейфов** — утилита для быстрого измерения сопротивлений шлейфов сигнализации		

	приборов, подключенных к АРМ «Орион», например, при проверке монтажа
	Мастер системы — утилита для архивирования БД, реставрации БД из архива, удаления устаревших данных, проверки целостности и модернизации базы данных
	Демонстратор работы приборов — утилита для эмуляции приборов, событий и настройки системы до установки на объект
	Место применения и связь с другим ПО
	Программное обеспечение АРМ «Орион Про» устанавливается и работает на одном персональном компьютере с организацией:
	• Основного рабочего места — дежурного оператора ИСО «Орион» с функциями контроля и управления системами охранной и пожарной сигнализации, контроля доступа, противопожарной автоматикой и видеонаблюдением
	• Вспомогательных рабочих мест:
	  ○ Администратора базы данных (ведение и корректировка базы ИСО «Орион»)
	  ○ Инженера наладчика (проверка шлейфов, эмуляция приборов и системы)
	  ○ Инженера по обслуживанию и эксплуатации (статистика системы, графики запыленности адресно-аналоговых пожарных извещателей, отчеты по служебным сообщениям и неисправностям)
	• Удаленных рабочих мест:
	  ○ Пост охраны с фотоверификацией
	  ○ РМ ответственного за контроль графика рабочего времени
	  ○ РМ ответственного за контроль работы дежурной смены		

31.	С2000М, пульт контроля и управления (или эквивалент) - Количество приборов и устройств ИСО «Орион», подключаемых к линии RS-485, не более 127	шт.	1

	- Интерфейс RS-4851 - Длина линии связи RS-485, м, не более 3000 - Интерфейс RS-232 - Длина линии связи RS-232, м, не более 20 - Количество шлейфов сигнализации и адресных извещателей, группируемых в разделы, не более 2048 - Количество управляемых в автоматическом режиме релейных выходов, не более 256 - Количество разделов, не более 511 - Количество групп разделов, не более 128 - Количество пользовательских паролей, не более 2047 - Объем журнала событий 1023 - Жидкокристаллический индикатор 2 строки х 16 символов, с подсветкой - Питание от резервированного источника постоянного тока - Напряжение питания, В от 10,2 до 28,4 - Рабочий диапазон температур, °С от +1 до +55 - Степень защиты оболочкой IP20 - Масса, кг, не более 0,3 - Габаритные размеры, мм 140х114х25 - Тип подключения к прибору клеммная колодка под винт, провод от 0,2 до 1,5 кв. мм		
32.	С2000-2, контроллер доступа (или эквивалент) - напряжение питания - от 10 до 15 В - потребляемый прибором ток в дежурном режиме - не более 100 мА - количество подключаемых считывателей - 2 - количество реле для управления запорными устройствами - 2 - максимальный коммутируемый ток реле - 5 А - максимальное коммутируемое напряжение реле - 30	шт.	5

	В - объём памяти Proximity-карт (ключей Touch Memory) - 4096 - объем буфера событий - 2047 - рабочий диапазон температур - от минус 30 до +50 °С - габаритные размеры - 150х103х35 мм		
33.	С2000-4, прибор приёмо-контрольный (или эквивалент) - работа в составе интегрированной системы охраны "Орион" - 4 шлейфа сигнализации со всеми видами охранных и пожарных извещателей -помехоустойчивость за счет селекции входного сигнала по длительности и фильтрации наводок 50 Гц -программирование типов шлейфов сигнализации: -охранные с распознаванием нарушения блокировочного контакта извещателя -пожарные "дымовые" и "тепловые" с распознаванием сработки одного и двух извещателей в шлейфе -пожарные комбинированные (дымовые и тепловые извещатели в одном шлейфе) -программирование параметров шлейфов под конкретный объект эксплуатации -возможность управления взятием/снятием под охрану или доступом одной Proximity-картой, или ключом Touch Memory -возможность управления взятием/снятием под охрану, доступом, выходными реле по интерфейсу RS-485 -программируемый временной график доступа -передача сообщений по интерфейсу RS-485 на пульт "С2000" или АРМ "Орион" -программируемая логика управления двумя реле ("С2000-4"), коммутируемая мощность 90 ВА -встроенный звуковой оповещатель ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ -напряжение питания – от 10,2 до 14,2 В или от 20,4	шт.	1

	до 28,0 В -потребляемый прибором ток в дежурном режиме – не более: -200 мА при напряжении питания 12 В -120 мА при напряжении питания 24 В -объем буфера событий - 255 -объем памяти Proximity-карт (ключей Touch Memory) - 2048 -рабочий диапазон температур - от минус 30 до +50 °С -габаритные размеры - 150 х 103 х 35 мм -"С2000-4-01" (охранный): нет реле, только охранные ШС, нет питания извещателей по ШС, нет контроля доступа, объем памяти ключей Touch Memory - 17, объем буфера событий - 10, напряжение питания - 12 В, ток потребления 70 мА -"С2000-4-02" (пожарный): нет реле, нет контроля доступа, объем памяти ключей Touch Memory - 17, объем буфера событий – 10, напряжение питания - 24 В, ток потребления 80 мА		
34.	USB-RS232, преобразователь интерфейса	шт.	1
35.	Извещатель магнитокотактный для металлических дверей	шт.	4
36.	Кнопка "выход"	шт.	4
37.	Считыватель Proxi-карт	шт.	11
38.	Proxi-карта бесконтактная	шт.	200
39.	Ростов-Дон Т-2 ММП, турникет-трипод электромеханический (или эквивалент) Напряжение питания турникета 12±2В постоянного тока Потребляемый ток, не более, 1,5А Пропускная способность в режиме однократного прохода 30-50 чел./мин. Габаритные размеры турникета (ширина×длина× высота) без штанг 180×412×990 мм, со штангами 745 х 780 х 990 мм	шт.	1

	Ширина перекрываемого прохода 745мм Допустимые статические усилия на середине преграждающей штанги, не более 100кгс Рабочий температурный диапазон от +1 °С до +40 °С Срок эксплуатации, не менее 8лет		
40.	Ростов-Дон штанга "антипаника" (или эквивалент) диаметр штанги 32мм материал - сталь с хромированным покрытием либо нержавеющая сталь длина до 700мм вес одной штанги 1,5 кг	шт.	3
41.	PERCo-BH01 2-00 (или эквивалент) - односторонняя стойка с двумя отверстиями предназначена для крепления патрубков; - габаритные размеры вертикальной стойки ограждения, мм Ø50х1000; - исполнение - нержавеющая сталь. Стойки и поручни выполнены из круглой трубы. Стыковка секций между собой возможна под любым углом	шт.	3
42.	PERCo-BH01 2-01 (или эквивалент) - двухсторонняя стойка с 4-мя отверстиями для крепления патрубков (угол между парами отверстий 180град.); - габаритные размеры вертикальной стойки ограждения, мм Ø50х1000; Исполнение - нержавеющая сталь. Стойки и поручни выполнены из круглой трубы. Стыковка секций между собой возможна под любым углом. Угол между парами отверстий 180 °	шт.	3
43.	PERCo-BH01 2-03 (или эквивалент) - трехсторонняя стойка с 6-ю отверстиями для крепления патрубков (углы между парами отверстий 90 и 180град.); - габаритные размеры вертикальной стойки	шт.	1

	ограждения, мм Ø50х1000;		
44.	PERCo-BH01 2-05, стойка с фиксатором поворотной створки с 2 отверстиями для патрубков (или эквивалент)	шт.	1
45.	PERCo-BH01 1-00, поручень диаметром 32мм длинной 915мм (или эквивалент)	шт.	4
46.	PERCo-BH01 1-01, поручень диаметром 32мм длинной 1415мм (или эквивалент)	шт.	6
47.	PERCo-BH01 1-05, поворотная створка "антипаника" длинной 1200мм с шарнирами (или эквивалент)	шт.	1
48.	PERCo-BH01 0-00, патрубок прямой для крепления поручней (или эквивалент)	шт.	24
49.	Источник бесперебойного питания 12В, 2А	шт.	5
50.	Источник бесперебойного питания 12В, 1,3А	шт.	1
51.	Аккумуляторная батарея 12В, 7 А/ч	шт.	6
52.	Автоматический выключатель 16А, с коробкой	шт.	6
53.	Колодка сетевая 3-х полюсная ~220В на 3 разъёма	шт.	1
54.	RJ 45, разъём для структурированных сетей связи	шт.	4
55.	UTP 2х2х0,52, провод монтажный	м	200
56.	МПВ 4х0,5, провод монтажный	м	50
57.	КСПВ 10х0,5, провод монтажный	м	30
58.	ШВВП 2х0,75, провод силовой	м	100
59.	Труба гофрированная 16	м	100
60.	Кабель-канал 15х10	м	60
61.	Кабель-канал 25х25	м	40
62.	Цементо-песочная смесь	кг	5
63.	Расходные материалы	к-кт.	8

Приложение 2

к техническому заданию

План холла в ОПФР по Белгородской области