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

Институт Физико-технический
Направление подготовки 14.04.02 Ядерные физика и технологии
Кафедра Физико-энергетические установки

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка и создание интегрированной системы безопасности на основе средств «BioSmart»

УДК 621.039.58:57.08

Студент

Группа	ФИО	Подпись	Дата
0АМ5Б	Вершинин Ярослав Антонович		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ФЭУ ФТИ	Степанов Б. П.	к.т.н.		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН ИСГТ	Верховская М.В.	к. экон. н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ПФ ФТИ	Гоголева Т.С.	к.ф.-м.н.		

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
ФЭУ	Долматов О.Ю.	к.ф.-м.н.		

Томск – 2017 г.

Планируемы результаты обучения

Код результата	**Результат обучения**
	Профессиональные компетенции
Р1	Применять глубокие, математические, естественнонаучные, социально-экономические и профессиональныезнания для теоретических и экспериментальных исследований в области использования ядерной энергии, ядерных материалов, систем учета, контроля и физической защиты ядерных материалов, технологий радиационной безопасности, медицинской физики и ядерной медицины, изотопных технологий и материалов в профессиональной деятельности.
Р2	Ставить и решать инновационные инженерно-физические задачи, реализовывать проектыв области использования ядерной энергии, ядерных материалов, систем учета, контроля и физической защиты ядерных материалов, технологий радиационной безопасности, медицинской физики и ядерной медицины, изотопных технологий и материалов.
Р3	Создавать теоретические, физические и математические модели, описывающие конденсированное состояние вещества, распространение и взаимодействие ионизирующих излучений с веществом и живой материей, физику кинетических явлений, процессы в реакторах, ускорителях, процессы и механизмы переноса радиоактивности в окружающей среде.
Р4	Разрабатывать новые алгоритмы и методы: расчета современных физических установок и устройств; исследования изотопных технологий и материалов; измерения характеристик полей ионизирующих излучений; оценки количественных характеристик ядерных материалов; измерения радиоактивности объектов окружающей среды; исследований в радиоэкологии, медицинской физике и ядерной медицине.
Р5	Оценивать перспективы развития ядерной отрасли, медицины, анализировать радиационные риски и сценарии потенциально возможных аварий, разрабатывать меры по снижению рисков и обеспечению ядерной и радиационной безопасности руководствуясь законами и нормативными документами, составлять экспертное заключение.
Р6	Проектировать и организовывать инновационный бизнес, разрабатывать и внедрять новые виды продукции и технологий, формироватьэффективную стратегию и активную политику риск-менеджмента на предприятии, применять методы оценки качества и результативности труда персонала, применять знание основных положений патентного законодательства и авторского права Российской Федерации.
	Общекультурные компетенции
Р7	Демонстрировать глубокие знания социальных, этических и культурных аспектов инновационной профессиональной деятельности.
Р8	Самостоятельно учитьсяи непрерывно повышать квалификациюв течение всего периода профессиональной деятельности.
Р9	Активно владеть иностранным языкомна уровне, позволяющем работать в иноязычной среде, разрабатывать документацию, презентовать результаты профессиональной деятельности.
Р10	Эффективно работать индивидуально и в коллективе, демонстрировать ответственность за результаты работы и готовность следовать корпоративной культуре организации.

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

Институт Физико-технический
Направление подготовки 14.04.02 Ядерные физика и технологии
Кафедра Физико-энергетические установки

УТВЕРЖДАЮ:
Зав. кафедрой ФЭУ
_____ _____ Долматов О.Ю.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	ФИО
0АМ5Б	Вершинину Ярославу Антоновичу

Тема работы:

Разработка действий модели нарушителя по преодолению инженерных средств физической защиты	
Утверждена приказом директора (дата, номер)	

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе	– нормативно-техническая документация – научно-технические источники
Перечень подлежащих исследованию, проектированию и разработке вопросов	– анализ нормативно-правовой базы по организации СФЗ на ЯО; – формирование требований к системе контроля и управления доступом на основе средств биометрической идентификации; – выбор технического оборудования и устройств учебной системы безопасности; – разработка и создание интегрированной системы безопасности с применением устройств биометрической идентификации «BioSmart»
Перечень графического материала	– структурная схема системы безопасности

Консультанты по разделам выпускной квалификационной работы

Раздел	Консультант
Финансовый менеджмент,	Верховская М.В.

ресурсоэффективность и ресурсосбережение	
Социальная ответственность.	Гоголева Т. С
Иностранный язык	Панамарёва А. Н.
Названия разделов, которые должны быть написаны на русском и иностранном языках:	
Проведение оценки эффективности СФЗ при её функционировании на ядерном объекте	
Способы описания последовательности действий нарушителя при преодолении ИТСФЗ	
Разработка возможных действий моделей нарушителя	
Оценка коммерческого потенциала и перспективности проведения исследования с позиции ресурсоэффективности и ресурсосбережения	
Безопасность использования и анализа данных при помощи электронной вычислительной машины	

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	6.02.2017

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. ФЭУ ФТИ	Степанов Б. П.	к.т.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ5Б	Вершинин Ярослав Антонович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
0АМ5Б	Вершинин Ярослав Антонович

Институт	Физико-технический	Кафедра	ФЭУ
Уровень образования	Магистратура	**Направление/специальность**	14.04.02 Ядерные физика и технологии/Ядерные реакторы и энергетические установки

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. *Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих*	Работа с информацией, представленной в российских и иностранных научных публикациях, аналитических материалах, статистических бюллетенях и изданиях, нормативно-правовых документах
2. *Нормы и нормативы расходования ресурсов*	
3. *Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования*	
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. *Оценка коммерческого потенциала, перспективности и альтернатив проведения НИ с позиции ресурсоэффективности и ресурсосбережения*	Оценочная карта конкурентных технических решений
2. *Планирование и формирование бюджета научных исследований*	Иерархическая структура работ SWOT-анализ Календарный план-график реализации проекта
3. *Оценка ресурсной, финансовой, социальной, бюджетной эффективности научного исследования*	Определение ресурсоэффективности проекта

Перечень графического материала *(с точным указанием обязательных чертежей)*

1. *Оценочная карта конкурентных технических решений*
2. *Матрица SWOT*
3. *Иерархическая структура работ*
4. *Календарный план проекта*
5. *Бюджет проекта*
6. *Определение ресурсоэффективности проекта*

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент каф. МЕН ИСГТ	Верховская М.В.	к.экон.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ5Б	Вершинин Ярослав Антонович		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
0АМ5Б	Вершинину Ярославу Антоновичу

Институт	Физико-технический	Кафедра	ФЭУ
Уровень образования	Магистр	**Направление/специальность**	14.04.02 Ядерные физика и технологии/ Ядерно-технический контроль и регулирование

Исходные данные к разделу «Социальная ответственность»:	
1. Описание рабочего места (рабочей зоны) на предмет возникновения:	– вредных факторов производственной среды (микроклимат, освещение, шумы, электромагнитные поля, ионизирующее излучение); – опасных факторов производственной среды (электрической, пожарной и взрывной природы).
2. Знакомство и отбор законодательных и нормативных документов по теме	– электробезопасность; – пожаробезопасность; – требования охраны труда при работе на ПЭВМ.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Анализ выявленных вредных факторов проектируемой производственной среды в следующей последовательности:	– воздействие на организм человека; – приведение допустимых норм; – предлагаемые средства защиты.
2. Анализ выявленных опасных факторов проектируемой произведённой среды в следующей последовательности:	– электробезопасность (в т.ч. статическое электричество, средства защиты); – пожаровзрывобезопасность (причины, профилактические мероприятия, первичные средства пожаротушения).

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент каф. ПФ ФТИ	Гоголева Т.С.	к.ф.-м.н.		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
0АМ5Б	Вершинин Ярослав Антонович		

Реферат

Выпускная квалификационная работа содержит 125 с., 16 рисунков, 10 таблиц, 24 источников, 3 приложения.

Ключевые слова: физическая защита, система контроля и управления доступом, ядерный объект, интегрированная система безопасности, биометрия.

Цель работы – создание системы безопасности на основе элементов и устройств биометрической системы «BioSmart».

В процессе работы был проведенанализ нормативно-правовой базы по организации СФЗ на ЯО,сформированы требования к системе контроля и управления доступом на основе средств биометрической идентификации, был произведен выбор технического оборудования и устройств системы безопасности.

В результате работы была разработана и создана интегрированная система безопасности с применением устройств биометрической идентификации «BioSmart».

Значимость работы заключается в развитии технической базы лаборатории «Систем физической защиты и противодействия ядерному терроризму» по обучению студентов вопросам функционирования СКУД СФЗ.

Выпускная квалификационная работа выполнена в текстовом редакторе MicrosoftOfficeWord 2016, иредакторе графикиAutoCAD 2014.

Обозначения и сокращения

АСУ – автоматизированная система управления

ИТСФЗ – инженерно-технические средства физической защиты

ПФЗ – предмет физической защиты

СКУД – система контроля и управления доступом

ИСБ – интегрированная система безопасности

ИКБ – интегрированный комплекс безопасности

СФЗ – система физической защиты

ТСФЗ – технические средства физической защиты

ЯМ – ядерный материал

ЯО – ядерный объект

Оглавление

Введение

В связи с развитием ядерной энергетики увеличивается количество опасных делящихся материалов и ядерного оборудования, также увеличивается число стран, обладающих ими.

Обеспечение безопасности объектов особой важности, использующих ядерные материалы и эксплуатирующих ядерные установки, на фоне роста террористических угроз является сегодня весьма актуальной задачей. Захват, вывод из строя ядерных установок или нарушение функционирования таких объектов чреваты катастрофическими последствиями,которые могут нанести крупный и невосполнимый ущерб государству, обществу.

Количество делящихся материалов на ядерных объектах возрастает, что связано с накоплением отработанного ядерного топлива. В связи с этим возрастает привлекательность ядерных объектов со стороны злоумышленников (нарушителей). ЯО нуждаются в тщательной и надежной охране периметра, пунктов хранения и использования ядерных материалов.

Для поддержания эффективного функционирования системы физической защиты необходимо ее обновлять, совершенствовать, так как современные террористы (нарушители) достаточно хорошо обучены, осведомлены, вооружены. Поэтому им должны быть противопоставлены высокоэффективные меры защиты. В качестве мер, по предотвращению террористических атак, в СФЗ совместно должны выполняться функции по обнаружению, задержке нарушителей и своевременному реагированию.

Реализация этих функций возможна только при создании автоматизированных систем физической защиты. Под автоматизированной системой понимают комплекс технических, программных, других средств и действий персонала, предназначенный для автоматизации процессов обеспечения безопасности объекта. Следовательно, для эффективного функционирования СФЗ необходима подготовка персонала, создание и применение современных, эффективных комплексов инженерно-технических средств физической защиты, способных дополнять друг друга.

Существует множество систем, выполняющих различные задачи по обеспечению безопасности. Однако ни одна из них не в состоянии гарантировать полной и надежной защиты предметов ФЗ, объектов и информации от всего спектра возможных угроз. Решение этой проблемы лежитв разработке интегральных комплексов, объединяющих различные подсистемы безопасности с общими техническими средствами, каналами связи, программным обеспечением, базами данных и др.

Основное достоинство интегрированных систем безопасности заключается в том, что все подсистемы взаимосвязаны, и в ответ на событие в одной подсистеме происходит соответствующее действие в другой. Появляется возможность задать требуемые сценарии реакции любой сложности на различные события.

Контроль доступа на базе считывателей биометрических параметров повышает уровень безопасности наиболее уязвимых мест на объекте. При этом безопасность обеспечивается не каким-то одним элементом системы, а комплексом организационных мер и технических средств СФЗ.

Для изучения процедуры биометрической идентификации, а также получения практических навыков по установлению и разграничению прав санкционированного доступа в помещения при работе с системой контроля и управления доступом, потребовалось создание системы безопасности.

Поэтомуцелью данной магистерской диссертации является созданиесистемы безопасности на основе элементов и устройств биометрической системы «BioSmart». Для достижения данной цели были сформулированы следующие задачи:

– анализ нормативно-правовой базы по организации СФЗ на ЯО;

– разработка системы безопасности с применением устройств биометрической идентификации «BioSmart»;

– выбор технического оборудования и устройств системы безопасности.

1Особенности построения и функционирования СФЗ ЯО

1.1 Требования к построению систем безопасности

Физическая защита на ядерном объекте представляет собой деятельность в области использования атомной энергии, осуществляемая в целях предотвращения диверсий и хищений в отношении ЯМ, ЯУ и пунктов хранения.

Цель ФЗ достигается путем создания и функционирования единой государственной системы организационных и технических мер, направленных на решение задач по обеспечению ФЗ на ЯО.

Для осуществления физической защиты на ядерном объекте создается и функционирует система физической защиты.

Основными задачами системы физической защиты ядерного объекта являются [2]:

– предупреждение несанкционированных действий;

– своевременное обнаружение совершения или попытки совершения несанкционированных действий – диверсии, хищения ЯМ, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя средств физической защиты;

– задержка проникновения нарушителя, замедление выполнения им любой поставленной цели - это время необходимо на ответную реакцию;

– пресечение несанкционированных действий (главная задача охраны, то есть силового вооруженного ответного действия);

– задержание лиц, причастных к подготовке и совершению диверсии или хищения ЯМ.

Система физической защиты включает в себя комплекс инженерно-технических средств, организационные и технические мероприятия, а также персонал, осуществляющий их применение и совершенствование.

Комплекс ТСФЗ должен решать следующие основные задачи [3]:

– сбор, обработку, анализ и контроль всей информации, получаемой от ТСФЗ;

– обеспечение возможности оценки тревожной ситуации в реальном масштабе времени;

– формирование и передачу сообщений (установленных сигналов) силам охраны, реагирования и органам управления СФЗ;

– обеспечение информационного взаимодействия между центральным пунктом управления (ЦПУ) и локальными пунктами управления (ЛПУ), а также с диспетчерскими пунктами и пунктами управления других систем безопасности ЯОО;

– выработку управляющих воздействий на управляемые физические барьеры и средства обеспечения функционирования СФЗ;

– контроль состояния и работоспособности ИТСФЗ;

– контроль действий и местоположения персонала при его работе с ЯМ и на ЯУ;

– хранение и выдача информации о функционировании СФЗ, попытках ее преодоления и несанкционированных действиях по отношению к защищаемым объектам и самим ИТСФЗ.

Создание, совершенствование и функционирование СФЗ ЯО проводится на основании единой системы планирования и координации деятельности по реализации комплекса организационных и технических мер физической защиты на ЯО [2].

Для выполнения задач физической защиты руководство ядерного объекта обеспечивает:

– анализ уязвимости ЯО;

– категорирование ПФЗ и ЯО;

– оценку эффективности СФЗ;

– работы по определению дальнейших путей совершенствования комплекса ИТСФЗ;

– оценку текущего состояния и сроков службы ИТСФЗ;

– опыт эксплуатации комплекса ТСФЗ;

– корректировку моделей нарушителей и угроз;

– изменение способов охраны и тактики действий сил реагирования;

– проведение учений по проверке и отработке взаимодействия в СФЗ;

– государственный надзор, ведомственный и административный контроль.

Бесперебойное и согласованное функционирование всех элементов СФЗ достигается:

– непрерывным и эффективным управлением силами и средствами СФЗ;

– разработкой и введением в действие в установленном порядке нормативных документов;

– подготовкой персонала службы безопасности, подразделений охраны и других подразделений ЯО к действиям в условиях штатных и чрезвычайных ситуаций;

– поддержанием в работоспособном состоянии технических средств физической защиты;

– регулярным и квалифицированным контролем соблюдения требований документов, регламентирующих вопросы обеспечения физической безопасности ЯО;

– постоянным отслеживанием изменяющейся оперативной обстановки, выявлением обстоятельств, ухудшающих защищенность ЯО, и адекватным реагированием на это;

– своевременным принятием действенных мер по устранению недостатков, выявленных в системе физической защиты.

В соответствии с последней редакцией НП 083-15:

– Контрольно-пропускные пункты должны оборудоваться средствами контроля и управления доступом, тревожно-вызывной сигнализации, обеспечения освещения и связи с пунктами управления системы физической защиты, караульным помещением и должностными лицами службы безопасности, а также техническими средствами (стационарными и переносными) для проведения досмотра людей и транспортных средств на предмет проноса (провоза) ядерных материалов и других запрещенных предметов;

– Обстановка на контрольно-пропускных пунктах должна контролироваться с помощью средств системы оптико-электронного наблюдения;

– Доступ через контрольно-пропускные пункты должен осуществляться с применением полноростовых пропускных устройств шлюзового или блокирующего типа;

– При использовании автоматизированных систем контроля и управления доступом должны применяться биометрические идентификационные признаки человека.

Исходя из последней поправки, можно сделать вывод о актуальности данной работы.

1.2 Обеспечение принципов при построении СФЗ

Для эффективного функционирования, согласно документу [2], построение СФЗ основано на совместном применении следующих принципов:

– зональное построение – обеспечение «эшелонированной защиты» предметов ФЗ. При организации зонирования объекта должно обеспечиваться усиление ФЗ от периферии к центру;

– равнопрочность – принятие мер и реализация мероприятий, направленных на создание условий, при которых эффективность системы физической защиты в части предотвращения «проектных угроз» является

примерно одинаковой для всех рассмотренных вариантов их развития. Равнопрочность должна быть обеспечена по всему периметру охраняемой зоны, включая контролируемые проходы и КПП. Требуемая эффективность СФЗ должна уточняться при создании и совершенствовании СФЗ с учетом категории ЯО и критерия «эффективность-стоимость»;

– надежность и живучесть – способность выполнять задачи в штатных и чрезвычайных ситуациях. Для этого проводится отбор и проверка благонадежности персонала ЯО, обучение и подготовка персонала службы безопасности ЯО и личного состава подразделений охраны к действиям в данных ситуациях;

– адаптивность – возможность адаптироваться СФЗ к изменениям:

угроз и моделей нарушителей, в конфигурации объекта и границ охраняемых зон, видов и способов охраны, размещения ПФЗ;

– регулярность контроля функционирования – путем проведения учений и оценки эффективности аналитическими и другими методами. Результат оценки эффективности должен использоваться для совершенствования СФЗ. Контроль обеспечения физической защиты осуществляется на ведомственном уровне и на уровне ЯО;

– адекватность, т.е. соответствие принятым угрозам и моделям нарушителя.

Последний принцип обеспечивается на ЯО путем:

– проведения анализа уязвимости;

– категорирования ЯО, ПФЗ, мест их хранения и использования;

– выбора структуры и состава комплекса ИТСФЗ;

– определение способов охраны и обороны ЯО;

– оценки эффективности СФЗ;

– использования при создании и совершенствовании СФЗ критерия «эффективность-стоимость».

При создании и совершенствовании системы физической защиты ядерного объекта в обязательном порядке:

– должны учитываться особенности объекта и действующие на нем меры ядерной, радиационной, экологической, пожарной, технической, информационной безопасности;

– ограничивается круг лиц, которые имеют доступ к ПФЗ, к элементам и системам, важным для обеспечения безопасности ядерного объекта или его системы физической защиты, к информации об организации, составе и функционировании системы физической защиты;

– обеспечивается соответствие СФЗ требованиям, установленным в отношении конкретного ядерного объекта;

– устанавливаются требования к организационно-техническим мерам по обеспечению ФЗ на объекте в зависимости от категории предметов физической защиты [1].

Таким образом, обеспечение физическая защита ЯМ. ЯУ и ПХ на объекте осуществляется комплексным использованием, а также взаимодействием всех ее составляющих частей СФЗ. При этом учитываются возможности дополнения работы отдельными подсистемами при обязательном выполнении собственных функций.

1.3 Организация санкционированного доступа на объект

1.3.1 Построение СКУД СФЗ ЯО

Система контроля и управления доступом (СКУД) предназначена для контроля и обеспечения санкционированного доступа персонала ЯОО (посетителей, командированных лиц) и транспорта в (из) помещения, здания, сооружения, зоны и территории в соответствии с установленной на объекте режимно-правовой средой.

Также СКУД должна обеспечивать исключение (или существенное затруднение)несанкционированного доступа нарушителей в охраняемые зоны и помещения. В случае обнаружения попыток несанкционированного доступа, а также в случае выявления факта силового воздействия на

элементы конструкций пропускных устройств и терминалов СКУД, данная информация должна быть в реальном времени предоставлена оператору.

Существующий ГОСТ [4] подразделяет СКУД в зависимости от:

- способа управления;
- числа контролируемых точек доступа;
- функциональных характеристик;
- вида объектов контроля;
- уровня защищенности системы от несанкционированного доступа.

В соответствии с [5] все СКУД условно делятся на четыре класса:

СКУД 1-го класса – это малофункциональная система малой емкости, работающая в автономном режиме и осуществляющая допуск всех лиц, которые имеют соответствующий идентификатор. Здесь используется ручной или автоматический способ управления исполнительными устройствами, а также световая или/и звуковая сигнализация.

СКУД 2-го класса – монофункциональная система. Могут быть как одноуровневыми, так и многоуровневыми. Система обеспечивает работу как в автономном, так и в сетевом режиме. Допуск лиц осуществляется по дате, временным интервалам. Данная СКУДобеспечивает автоматическое управление исполнительными устройствами.

СКУД 3-го и 4-го классов по своей структуре сетевые. В данных системах используются различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей карт *Wiegand* или магнитных карт, специализированные интерфейсы и др.) и более сложные идентификаторы.

Данный вид СКУД используется в случае необходимости контроля времени прохода сотрудников и посетителей на объект и в помещения. Также применяются более сложные электронные идентификаторы (*Proxmity*, карточка *Wiegand*, биометрический контроль или их сочетания).

Системы 3-го класса, как правило, интегрируются с системами ОПС и ТСВ на релейном уровне. Такой способтребует наличие дополнительного модуля в контроллере (дополнительных входов/выходов в контроллере), куда

будут подключаться охранные или пожарные извещатели, а также релейные выходы для управления камерами и другими устройствами. Данный вид интеграции применяется в основном на небольших объектах. В данном случае количество взаимодействий между системами невелико и все они учитываются в процессе проектирования системы безопасности.

Системы 4-го класса – многоуровневая система большой емкости. Отличительная особенность больших систем – наличие программного обеспечения, которое позволяет реализовать большое число функциональных возможностей и высокую степень интеграции на программном (системном) уровне с другими системами охраны и безопасности.

1.3.2 Выполняемые функции и предъявляемые требования к СКУД

Основной задачей СКУД, как ее подсистемы СФЗ, является своевременное обнаружение и предупреждение несанкционированных действий (несанкционированного прохода, выноса ЯМ и проноса (провоза) запрещенных предметов).

Настройка прав доступа лиц на объект осуществляется с использованием следующих параметров:

– уровень доступа;

– режим контроля повторного прохода (*anti-passback*) – защита от повторного использования идентификатора для прохода в одном направлении;

– «правило двух лиц» – принцип групповой работы, который основан на требовании одновременного присутствия на одном рабочем месте не менее двух человек, обладающих соответствующими полномочиями.

Основные тактико-технические и функциональные требования, применяемые к средствам СКУД, это [3, 4, 5]:

– исключение возможности проникновения на объект и выхода с объекта лиц без выполнения ими режимных процедур, установленных на объекте;

– высокая достоверность идентификации личности;

– обеспечение максимальной пропускной способности КПП при минимальной численности личного состава, несущего боевую службу на них;

– обеспечение высокого качества досмотра транспорта и проверки пропусков;

– безопасность эксплуатации, устойчивость к климатическим условиям и удобство обслуживания.

Для построения и разграничения прав санкционированного доступа на ядерном объекте устанавливается несколько рубежей защиты, расположенных последовательно на пути продвижения нарушителя к цели и обеспечивающих эшелонированную защищенность ПФЗ.

Основной принцип построения СКУД – усиление требований по контролю права доступа лиц в направлении от защищенной к вложенным зонам – внутренней и особо важной. Для защищенной зоны контроль доступа проходящих лиц на КПП осуществляется с применением турникетов, обеспечивающих задержание лиц, не имеющих прав доступа. В автоматизированных СКУД широко используются способы удостоверения личности по присвоенным признакам. Контроль доступа проходящих во внутреннюю зону лиц помимо пропускных устройств может осуществляться с применением присвоенных индивидуальных признаков либо присущих человеку биометрических признаков. Все операции, производимые в особо важной зоне, осуществляются с соблюдением правила двух (трех) лиц (доступ в зону и из нее, доступ в отдельные помещения, сооружения, здания, снятие с охраны/постановка под охрану и т.д.).

Для контроля доступа проходящих лиц необходимо использовать биометрические способы удостоверения личности, применяемые совместно с

присвоенными человеку признаками. При выполнении работ с ПФЗ категории А или Б, а также при осуществлении доступа в помещения категории А или Б требование данного пункта является обязательным [2]. Контроль доступа проходящих лиц в дополнение к вышеназванным требованиям может осуществляться либо с применением присвоенных индивидуальных признаков, либо присущих человеку биометрических признаков.

1.4 СКУД на основе устройств биометрической идентификации

В соответствии с [2], при осуществлении доступа в помещение категории А или Б требуется использовать биометрические системы контроля доступа.

Огромный интерес к биометрии обусловлен рядом объективных причин. В классических парольных системах, а также системах на основе карт доступа подглядывание или угадывание пароля, кража или изготовление дубликата карты приводит к компрометации всей системы. Более того, законный пользователь, потеряв или испортив карту, теряет возможность доступа к системе. Системы на основе биометрии практически лишены этих недостатков – идентификатор неразрывно связан с самим пользователем, поэтому потеря или изменение идентификатора возможны только в чрезвычайных происшествиях, а современные сканеры биометрических данных позволяют обнаруживать попытки использования муляжей.

В отличие от аутентификации пользователей по паролям или уникальнымцифровым ключам, биометрические технологии всегда вероятностные, поскольку всегда есть шанс совпадения сравниваемых биологических характеристик у двух разных людей. В силу этого любая биометрическая система содержит следующие два параметра [6]:

– ошибка первого рода (*FalseRejectionRate, FRR*) – вероятность того, что легитимный пользователь может быть не распознан системой.

Приемлемым уровнем ошибок первого рода в современных биометрических системах является 1%;

– ошибка второго рода (*False Acceptence Rate, FAR*) – вероятностьошибочной аутентификации (идентификации) нелегитимного пользователя. Современные системы биометрической аутентификации позволяют достигать уровней ошибок второго рода менее, чем 0.00001%.

Ошибки первого и второго рода в первую очередь связаны с технической невозможностью получения всегда одинаковых цифровых образов данной биометрической характеристики при каждом ее сканировании. Шумы в датчике, различное положение частей тела человека при сканировании, искажения самих характеристик (мимика, ожоги или порезы пальцев, световые блики и т.п.) – все это отражается на формируемом цифровом образе.

1.5 Интегрированная система безопасности с использованием устройств биометрической идентификации

1.5.1 Интегрированная система безопасности. Назначение и состав

Системы защиты постоянно развиваются. Развивается все: средства идентификации, системы видеонаблюдения, системы контроля и управления доступом. Кроме того, некоторые составные элементы комплекса технических средств физической защиты объекта со временем морально устаревают, что не дает им выполнять свои функции при обеспечении СФЗ. Анализ возможностей СКУД показывает, что нет ни однойсистемы, готовой обеспечить в одном лице все необходимые требования для ТСФЗ на ЯО.Логическим выводом является интеграция подсистем в одно целое.Решением такой задачи явилось создание интегрированных систем безопасности с широкими функциональными возможностями, позволяющими автоматизировать также управление инженерными системами здания или объекта. Основой таких ИСБ служит единая аппаратно-программная платформа, представляющая собой автоматизированную систему управления с многоуровневой сетевой структурой, имеющую общий центр управления на базе локальной компьютерной сети и содержащую линии коммуникаций, контроллеры

приема информации, управляющие контроллеры и другие периферийные устройства, предназначенные для сбора и обработки информации от различных датчиков (в том числе от извещателей пожарной и охранной сигнализации), а также для управления различными средствами автоматизации (оповещение, противопожарная автоматика и пожаротушение, инженерные системы и т.д.).

ИСБ представляют собой автоматизированную систему управления, обеспечивающую управление безопасностью различных объектов,следовательно, на нее в полной мере распространяются положения «Комплекса стандартов и руководящих документов на автоматизированные системы». Согласно [7], установлены следующие общие понятия.

Автоматизированная система – система, в которую входит персонал и комплекс средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Интегрированная автоматизированная система–совокупность двух или более взаимоувязанных АС, в которых функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС.

В соответствии с этими терминами выделим понятие об интегрированной системе безопасности.

Интегрированная система безопасности– совокупность технических средств (двух или более взаимоувязанных АС), предназначенных для построения системохранной,пожарнойсигнализациииоповещения, управления противопожарной автоматикой, контроля иуправлениядоступоми системтелевизионногонаблюдения, которые обладают технической, информационной, программной и эксплуатационной совместимостью так, что эту совокупность можно рассматривать как единую АС.

Из этого определения также следует, что ИСБ это система, обеспечивающая защиту от нескольких видов угроз. В данном выше определении – ИСБ предназначена для защиты от пожара (пожарная

сигнализация, оповещение, противопожарная автоматика) и от криминальных угроз (охранная сигнализация, контроль доступа, охранное телевидение).

Современные интегрированные системы безопасности обеспечивают максимальную функциональность применения комплекса технических средств.

Составными частями ИСБ являются:

– сеть датчиков, позволяющая получить максимально полную информацию со всего пространства, которое находится в поле зрения службы безопасности, позволяет воссоздать на центральном пункте наблюдения всестороннюю и объективную картину состояния помещений и территории объекта и работоспособности всей аппаратуры и оборудования;

– исполнительные устройства, при необходимости действующие автоматически или по команде оператора;

– пункты (или пункт) контроля и управления системой отображения информации, через которые оператор может следить за работой всей системы в пределах своих полномочий;

– центральный процессор с программирующим устройством, наглядно представляющий информацию датчиков и накапливающий ее для последующей обработки;

– коммуникации, посредством которых обеспечен обмен информацией между элементами системы и ее операторами.

Такая структура интегрированной системы безопасности позволяет:

– контролировать большое количество помещений с созданием нескольких рубежей защиты;

– обеспечивать иерархический доступ сотрудников и посетителей в помещения и четко разграничивать полномочия по праву доступа в помещения и по времени суток и по дням недели;

– идентифицировать личность человека, который пересекает рубеж контроля доступа;

– следить за точным исполнением персоналом охраны своих служебных обязанностей;

– предупредить попадание на объект запрещенных материалов, веществ, оружия и устройств;

– взаимодействовать посту охраны и органам правопорядка при несении охраны и в случае локализации происшествий;

– накопить документальные материалы для использования их при расследовании и при анализе происшествий;

– обеспечить оперативный инструктаж работников системы о порядке действий в различных штатных и нештатных ситуациях благодаря автоматическому выводу на монитор текста инструкций в нужный момент.

Кроме того, гибкость программированияразличных функций интегрированной системы способствует противодействию такихдействий, как прерывание каналов передачи тревожной информации, частичной нейтрализации системы людьми, имеющими доступ к ее элементам. Также это препятствует проникновению с сигналом тревоги и последующим уничтожением информации о происшествии, использованию отклонений от предписанного порядка несения службы персоналом охраны, созданию нештатных ситуаций в работе системы.

1.5.2 Структура интегрированной системы безопасности и принципы ее построения

Согласно [8,9], современные ИСБ строятся на основе иерархической сетевой структуры, в которую входят компьютерные сети, а также локальные сети различного уровня сложности специальных вычислительных устройств – контроллеров.

Обобщенная структура ИСБ приведена на рисунке 1. В ней можно выделить четыре уровня сетевого взаимодействия.

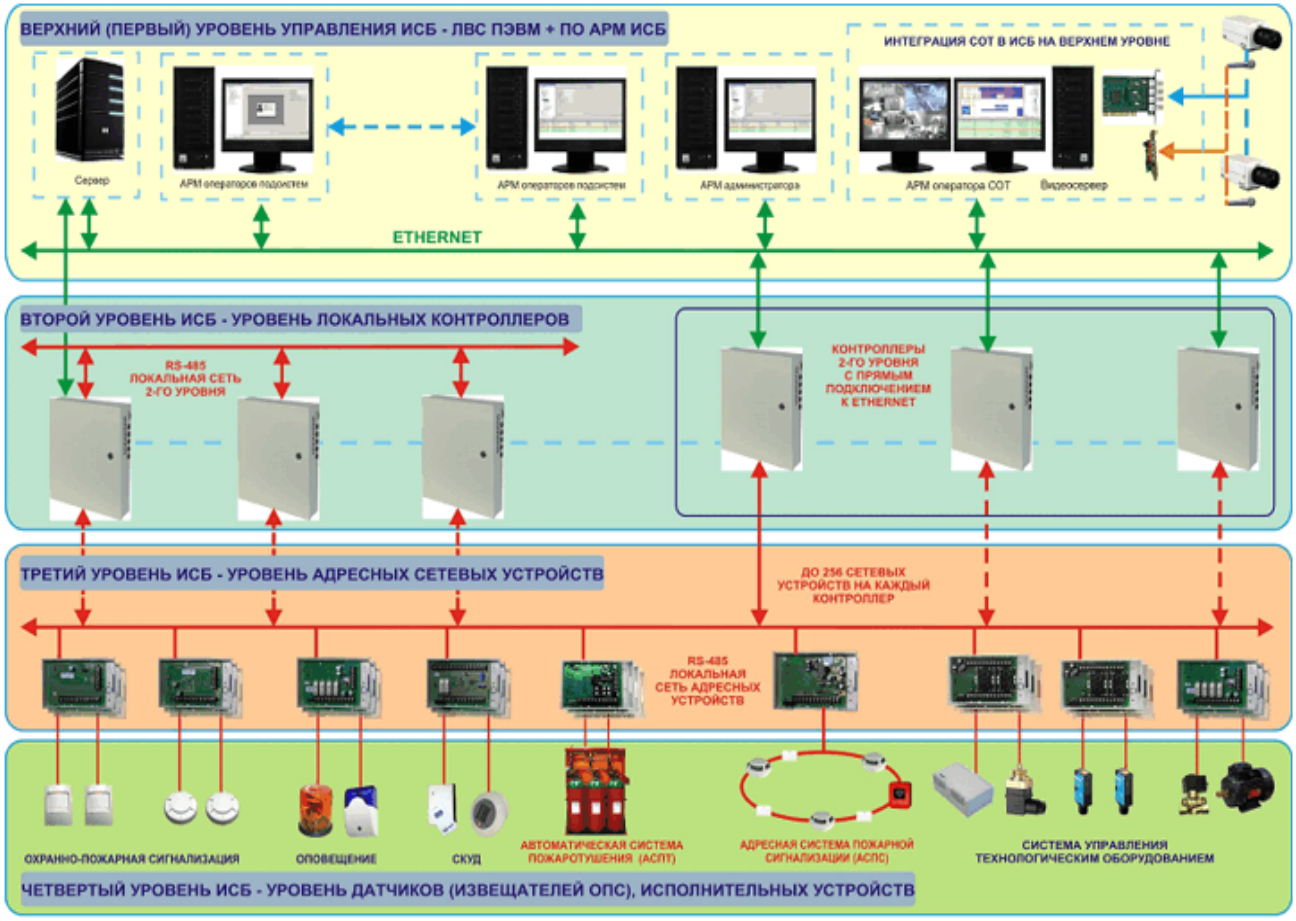

Рисунок 1– Обобщенная структура ИСБ

Первый(верхний) уровень представлен в виде компьютерной сети типа клиент/сервер на основе сети *Ethernet*, с протоколом обмена *TCP/IP* и с использованием сетевых операционных систем. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов. Управление ИСБ на верхнем уровне обеспечивается посредством специализированного программного обеспечения (СПО). Для небольших объектов возможно использование для управления ИСБ одного компьютера. На верхнем уровне также обеспечивается связь и управление удаленными объектами. Современные возможности компьютерных сетей позволяют передавать информацию по различным каналам связи, тем самым на основе ИСБ можно создавать системы мониторинга безопасности удаленных объектов.

Второйуровень – уровень локальных контроллеров, основных компонентов управления ИСБ. Каждый локальный контроллер должен

обеспечивать выполнение основных функций в своей зоне контроля, даже при нарушении связи с верхним уровнем ИСБ. Для связи между однородными контроллерами (горизонтальный уровень связи) используется интерфейс *RS*485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. Связь между вторым и верхним уровнем (вертикальный уровень связи) может обеспечиваться через один из сетевых контроллеров, посредством подключения его к серверу ПО АРМ ИСБ через стандартный порт ПЭВМ. В контроллерах некоторых ИСБ возможен прямой выход на первый уровень в протоколе *TCP/IP*.

Третийуровень – уровень адресных сетевых устройств, которые подключаются к каждому контроллеру второго уровня. Здесь, как правило, применяется интерфейс *RS*485. Количество сетевых устройств, подключаемых к одному контроллеру, может быть до 256.

Четвертый уровень –считыватели и исполнительные устройства СКУД, датчики и устройства управления технологическим оборудованием и др.Обычно здесь применяются специализированные интерфейсы и протоколы.

Технические возможности ИСБ позволяют определить дальнейшие перспективы их развития – интеграция с другими системами автоматизации и расширение видов и количества угроз, защита от которых обеспечивается с помощью ИСБ.

Процесс создания системы безопасности объекта включает в себя ряд этапов, основные из которых это проектирование, монтаж, пуско-наладочные работы, сдача в приемку заказчику.

Каждый объект, на котором создается система безопасности, является уникальным, поэтому каждая проектируемая система представляет собой продукцию единичного производства, создаваемую заново для каждого конкретного объекта. При создании такой системы нужно учитывать положения [10].

Важнейшую роль при создании системы играет процесс проектирования, так как на этапе проектирования закладываются все необходимые качественные характеристики системы. При проектировании важным вопросом является выбор технических средств ИСБ, из которых будет создаваться система.

ИСБ в любом случае представляет собой сложную техническую систему и при ее создании приходится использовать различное оборудование, как по функциональному назначению, так и оборудование разных производителей. При этом всегда встает задача совместимости оборудования. Причем она включает в себя две составляющие. Первая это задача обеспечения взаимодействия оборудования различных подсистем, объединенных в ИСБ. Вторая – совместимость оборудования разных производителей. Эти задачи должны быть решены на этапе проектирования ИСБ и могут быть оптимизированы в рамках выбора способа (платформы) интеграции.

Принципы проектирования ИСБ во многом определяются способом интеграции, который можно разбить на четыре основных уровня (платформы интеграции) [11]:

- интеграция на проектном уровне (проектная платформа) – объединение разнородного оборудования, специально не предназначенного для построения ИСБ, только на этапе проектирования системы;
- интеграция на программном уровне (программная платформа) – объединение оборудования разных производителей, на базе специально разработанного для интеграции программного продукта и управления системой на базе ПЭВМ общего назначения;
- интеграция на аппаратно-программном уровне (аппаратно-программная платформа)–объединение оборудования и программного продукта единого производителя и управления системой на базе ПЭВМ;
- интеграция на аппаратном уровне (аппаратная платформа)– объединение оборудования и программного продукта единого производителя

и управления системой без использования ПЭВМ общего назначения, на основе специализированных высокопроизводительных контроллеров и ЛВС на их основе.

Особо следует отметить интеграцию в ИСБ подсистемы видеонаблюдения. Причем следует, прежде всего, рассматривать цифровые технологии в системах охранного телевидения (СОТ), как наиболее перспективные. Особенности интеграции СОТ связаны с тем, что для передачи и обработки видеоданных в цифровых СОТ требуются значительные вычислительные и информационные ресурсы, поэтому реализация цифровых СОТ в ИСБ возможна только на верхнем уровне управления.

Рассмотрим более подробно первый вид интеграции – интеграция на проектном уровне.

Объединение (интеграция) этих систем осуществляется путем установки оборудования управления подсистемами в общем помещении – центральном пункте управления. Взаимодействие между подсистемами осуществляется на уровне операторов подсистем, то есть без автоматизации.

Очевидно, что это минимальный уровень интеграции, ему присущи известные недостатки («человеческий фактор», разнородность аппаратуры, сложность обслуживания, параллельность прокладываемых коммуникаций, отсутствие автоматизации и т.д.) и его нельзя считать в настоящее время перспективным, хотя имеется ряд фирм, которые предлагают свои готовые и проверенные проектные решения.

Оптимальным подходом в этом случае, следует считать разработанную фирмой – проектировщиком собственную проектную методологию построения систем.

Вторым видом – интеграция на программном уровне.

В этом случае роль объединения подсистем играет специальное программное обеспечение (СПО) – программный пакет, разработанный и поставляемый как самостоятельный продукт (программная продукция

серийного производства, специально предназначенная для интеграции технических подсистем). Такое СПО предназначенное для функционирования в аппаратной среде, как правило, в локальной сети ПЭВМ общего назначения, которая представляет собой верхний уровень ИСБ. Сопряжение с аппаратной частью подсистем нижнего уровня осуществляется с помощью программ-драйверов, разрабатываемых специально для поддержки конкретных средств других производителей. Связь с аппаратными средствами осуществляется с помощью стандартных портов ПЭВМ.

Подобное построение ИСБ имеет ряд положительных сторон. Это возможность на программном уровне, используя все возможности современных компьютерных технологий, создавать высококачественные многофункциональные программные системы. Возможность интеграции с аппаратными средствами других производителей (при наличии соответствующего драйвера и соответствующих интерфейсов обмена данными в самих применяемых средствах).

С другой стороны, это порождает и определенные недостатки – необходимость разработки драйверов для каждого применяемого аппаратного средства. При этом не всегда разработчик аппаратного средства предоставляет протоколы обмена данными. Даже, если протоколы открыты и документированы, в них могут быть заложены ограниченные возможности, не позволяющие оптимальным образом обеспечить сопряжение. Кроме того, фирма разработчик программной системы, поставляя только свой программный продукт, не может в этом случае в полном объеме гарантировать работу всей системы в целом.

Следующий вид – интеграция на аппаратно-программном уровне.

В этом случае аппаратные и программные средства разрабатываются в рамках единой системы. Это позволяет достигнуть оптимальных характеристик, так как вся разработка сосредоточена, как правило, в одних

руках и система как законченный продукт поставляется с полной гарантией производителя.

В данном случае основой для построения ИСБ служит продукт серийного производства – комплекс (набор) аппаратно-программных средств, которые обладают технической, информационной, программной и эксплуатационной совместимостью.

Задача проектировщика при выборе аппаратно-программной платформы интеграции заключается только, в основном, к адаптации комплекса для конкретного объекта. Эта задача может быть еще более оптимизирована, если разработчик комплекса аппаратно-программных средствдля построения ИСБ предлагает набор типовых проектных решений. При этом возможно также получить оптимальные технико-экономические показатели.

Общим недостаткомприведенных выше способов интеграции является использование на верхнем уровне управления ИСБ персональных компьютеров общего назначения. Известно, что ПЭВМ и базовое ПО общего назначения (операционные системы, системы управления базами данных и др.) предназначены, в основном для офисного и бытового применения. Они обладают излишней функциональностью и недостаточной надежностью для решения задач автоматизации управления системами, в особенности системами безопасности.

Для использования в ИСБ необходимо применять специализированные промышленные ПЭВМ и соответствующее специализированное базовое ПО. Однако стоимость такого решения существенно выше.

Последним в перечне видов –аппаратная платформа интеграции.

Аппаратная платформа интеграции – относительно новое направление развития принципов построения ИСБ. При разработке данного направления ставилась задача устранения общего недостатка других методов интеграции,

то есть отказ от использования в ИСБ на всех уровнях ПЭВМ общего назначения.

Аппаратный способ интеграции – на основе оборудования без участия ПЭВМ, обеспечивает максимальную надежность и быстродействие системы.

Для замены ПЭВМ в составе ИСБ на верхнем уровне управления используется специально разработанный для этой цели универсальный контроллер с высокими вычислительными возможностями. Такой контроллер может служить основой для создания интегрированных систем комплексной безопасности и жизнеобеспечения.

Особенность аппаратной платформы заключается в том, что все элементы интегрированной системы безопасности, включая функционал верхнего уровня (АРМ оператора), реализованы в одном приборе по технологии *SystemInBox*.

Прибор должен обеспечивать непосредственное подключение и реализацию алгоритмов функционирования всех подсистем ИСБ: охранная и пожарная сигнализация, управление исполнительными устройствами, управление пожаротушением, контроль и управление доступом, видеонаблюдение, диспетчеризация и технологический мониторинг. И, главное, должна обеспечиваться возможность организации АРМ оператора системы без использования дополнительного компьютера: графический монитор, клавиатура, мышь должны подключаться непосредственно к прибору.

1.5.3 Совместное применение устройств СОЭН и системы контроля и управления доступом в СФЗ

СОЭН применяется для удаленного наблюдения за зданиями, сооружениями, периметром ЯО. Целью применения данной системы, является оценка ситуации в реальном времени, наблюдение за продвижением и действиями нарушителя, корректировка действий персонала системы ФЗ.

Система оптико-электронного наблюдения, является составной частью комплекса ТС ФЗ, поэтому она служит одним из важных дополнений СФЗ. Задачи, выполняемые системой оптико-электронного наблюдения, отмечены на рисунке 2.

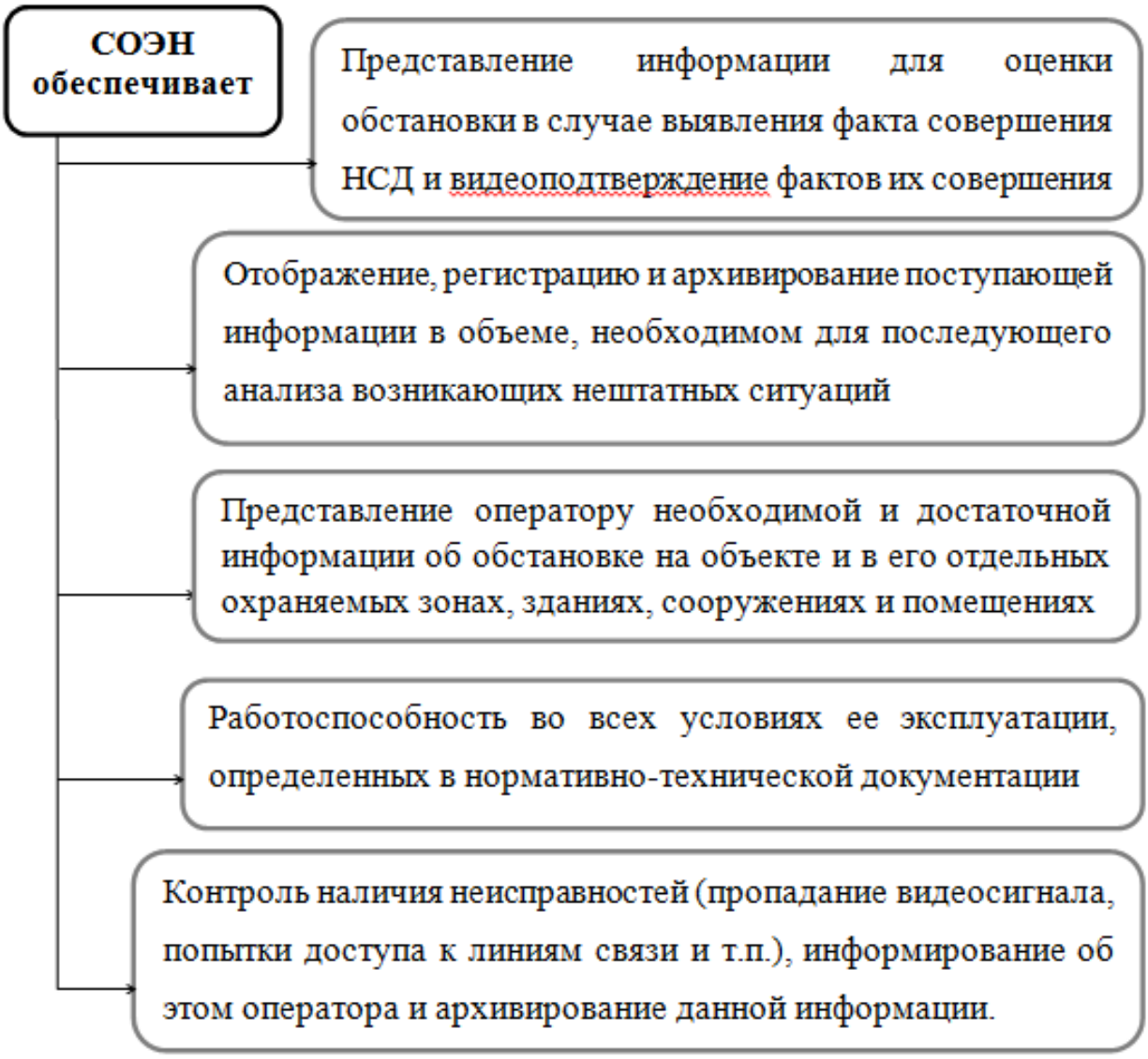

Рисунок 2-Задачи СОЭН

Основной задачей, выполняемой системой оптико-электронного наблюдения следуя из рисунка 2, являетсяпредставление оператору необходимой и достаточной информации об обстановке на объекте и в его отдельных охраняемых зонах, зданиях, сооружениях и помещениях.

При получении данной информации оператор ЦПУ может корректировать работу СКУД. Система контроля и управления доступом предназначенадля затруднения и предотвращения несанкционированного

доступанарушителей на ЯО (территорию, здания, помещения, прилегающие сооружения) [1]. Назначение СКУД отображено на рисунке 3.

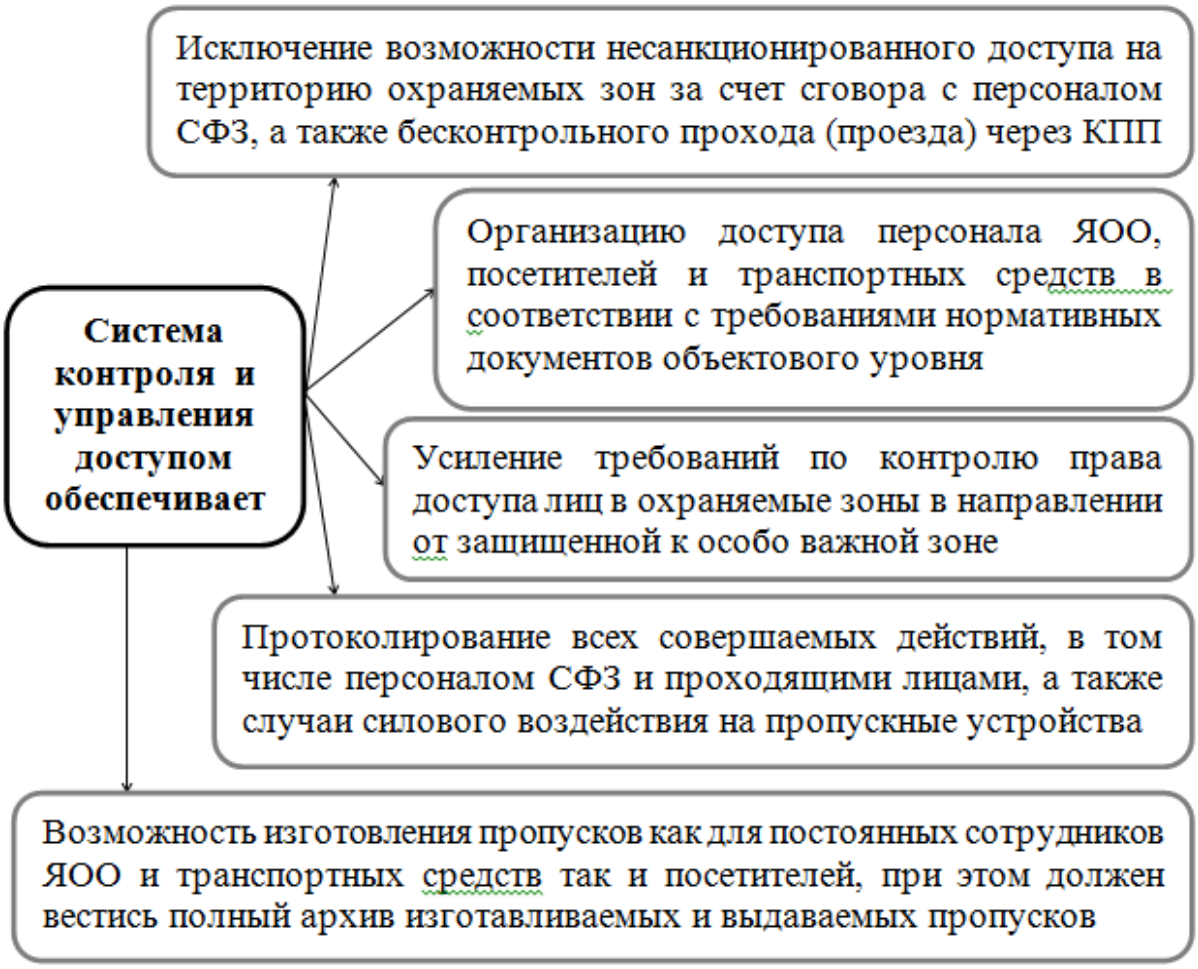

Рисунок 3-Назначение СКУД

Для получения доступа к зданиям, помещениям, ПХ ЯМ на ядерном объекте, требуется высокая точность идентификации личности. В качестве основных средств идентификации в СКУД применяются биометрические сканеры, считывающие биометрические характеристики человека – это черты лица, отпечатки пальцев, рисунок радужной оболочки глаз или вен на руке. Точность полученных данных, в результате сканирования, составляет до 99,9% (то есть одна ошибка позитивной идентификации на тысячу распознаваний).

Чтобы убедиться в том, что личность, пытающаяся получить доступ в помещение, не выдает себя за другого человека, обычно применяются иные способы идентификации: карты доступа, электронные пропуска, цифровые

коды. Подделать перечисленные способы идентификации личности, для опытных злоумышленников, не составляет большого труда. В связи с этим, установка системы видеонаблюдения позволила бы свести к минимуму процент ложного распознавания личности. А применение анализа видеоизображения в системе видеонаблюдения позволило бы автоматизировать процесс идентификации.

Рассмотрим возможность применения системы видеонаблюдения с функцией анализа видеоизображения, совместно со СКУД на следующем примере. Камера видеонаблюдения устанавливается на подходе к охраняемому помещению, оснащенного биометрическими сканерами и электромагнитным замком. Человек, направляющийся к рассматриваемому помещению, попадает в поле зрения видеокамеры. Камера, получает изображение и передает его на рабочее место оператора, где происходит анализ видеоизображения. В процессе анализа из полученного изображения выделяется лицо человека. Далее, в автоматическом режиме, происходит сравнение биометрических параметров захваченного лица с теми, которые хранятся в заранее созданной базе данных лиц.

По завершению сравнения лиц оператору ЦПУ на монитор выводятся результаты поиска. В результатах могут содержаться все данные о человеке (Фамилия, Имя, степень допуска и т.д.). Так же личность может быть отмечена, как нежелательный посетитель. По этим характеристикам оператор принимает решение о том, что предоставить либо запретить доступ в рассматриваемое помещение.

В связи с развитием технологийвозможности анализа видеоизображения расширяются. Благодаря чему вскоре систему видеонаблюдения и систему контроля и управления доступом можно будет полностью автоматизировать.В этом случае оператор ЦПУ будет лишь контролировать операции, выполняемые данной системой.

1.5.4Методы идентификации

Для выполнения основных задач СФЗ при осуществлении контроля прав доступа сотрудников на ЯО системе контроля и управления доступом необходимо однозначно определить: имеет ли данный человек право санкционированного прохода на объект через определенную точку доступа.

В этом случае сотруднику требуется идентифицировать себя (пройти процесс отождествления личности с одним из известной системы признаков. При этом система определяет, кто есть человек, предъявивший системе идентификатор, и имеет ли он права на санкционированных проход).

Аутентификацией в свою очередь является проверка соответствия личности по идентификатору, который предъявляется.

В аппаратно-программных средствах СКУД, разница между процедурами идентификации *и* аутентификации следующая: при процессе идентификации система анализирует всю базу данных зарегистрированных пользователей, сравнивая уже имеющиеся записи с полученными. Если такая запись найдена, то система начинает определять уровень допуска, а также и другую информацию о субъекте. При аутентификации идентификатор субъекта уже известен, и чтобы подтвердить его личность, системе требуется выполнить единственное действие – проверить соответствие дополнительно вводимых данных с уже имеющимися данными о пользователе в базе данных. Приведенные процедуры сейчас широко используются в биометрических системах идентификации.

Основными проблемами, связанными с применением средств идентификации в СКУД, являются возможность их потери или кражи. Не исключена возможность изготовления злоумышленниками копии идентификатора.

Среди существующих идентификаторов, используемых в СКУД СФЗ, можно выделить следующие (размещены по степени увеличения надежности) [12]:

– персональный идентификационный номер;

– магнитные карты;

– *wiegand* карты;

– *proximity*-карты;

– биометрические характеристики.

Персональный идентификационный номер представляет собой комбинацию цифр или букв, которая предъявляется системе для определения прав доступа. Недостатки – сотрудник может сообщить свой пароль постороннему лицу, забыть комбинацию, возможен подбор пароля нарушителем. Достоинства – низкая стоимость, удобство для пользователей.

Магнитная карта контактная карта с магнитной полосой, на которой записан код. Данный вид идентификатора является бюджетным, но далеко не надежным – код, записанный на дорожках магнитной полосы, легко может быть перепрограммирован. Недостаткам магнитной карты является механический контакт при процедуре считывания, который сокращает срок службы. Также присутствует необходимость аккуратного обращения, связанного с возможностью потери или повреждения информации. Такие искажения могут быть вызваны как слабыми магнитными полями, так и небольшим отклонением от приемлемого для эксплуатации температурного диапазона и уровня влажности воздуха.

Карта *Wiegand* – контактнаякарта с содержащимися внутри тонкими металлическими проволочками, расположенными в определенном порядке, представляющем собой кодовую комбинацию. Такой тип карт стоек к воздействиям электромагнитного поля, а также к высоким температурам. Вероятность подделки крайне мала. Все электронные компоненты считывателей покрыты специальным защитным слоем, что позволяет использовать их как внутри помещений, так и снаружи. К недостаткам можно отнести хрупкость карт и возможность повреждения при изгибе. Код карте присваивается при изготовлении и в дальнейшем отсутствует возможность его изменения.

Proximity-карта – бесконтактнаякарта с расположенной внутри микросхемой с записанной информацией. Радиочастотным способом информация с карты считывается на расстоянии от 4 до 85 см (расстояние считывания автомобильных идентификаторов достигает нескольких метров). Достаточно надежные и более удобны в эксплуатации (возможно скрытное размещение считывателя за неметаллической стенкой). К недостаткам следует отнести невозможность работы при воздействии сильных электромагнитных полей. Данный тип карт используется в тех случаях, когда требуется обеспечение высокой пропускной способности, скрытности места установки считывателя или для дистанционного контроля доступа.На карту наносится фотография владельца, фамилия, имя и отчество, занимаемая должность или другая служебная информация, которая позволит службе безопасности идентифицировать владельца правильно.

В различных источниках иногда используется следующее название технологии – система радиочастотной идентификации и регистрации объектов (*RFID*-системы). Также они способны осуществлять идентификацию, используя уникальный цифровой код, излучаемый электронной меткой-транспондером, закрепленной на объекте. По способу питания бывают активные (питание идет от встроенной батареи) и пассивные транспондеры. По типу организации памяти транспондеры бывают *RO* (*ReadOnly*), на которых записан уникальный заводской код, и *R/W* (*Read/Write*) транспондеры, в которые код вносится пользователем, многостраничные транспондеры с пользовательской памятью объемом до 1 кБ, а также транспондеры с «плавающим» кодом, защищающим память. Различие систем различаются в несущей частоте используемых сигналов, типе модуляции, протоколе радиообмена, объеме возвращаемой транспондером информации.

Биометрические системы идентификациибоее эффективны, так как в качестве идентификатора используются не физические носители, а персональная информация, уникальная для каждого человека. В настоящее

время системы контроля и управления доступом, основанные на данной технологии, лидируют не только в эффективности, но и в удобстве установки и последующей эксплуатации. У всех биометрических устройств специфические требования к аппаратным и программным средствам. Пользователи должны быть зарегистрированы, чтобы пройти аутентификацию.

Все методы биометрической идентификации разделяются на статические методы, принцип работы которых основан на физиологических характеристиках человека, данных ему от рождения и обладающих уникальными свойствами, а также динамические методы, базирующиеся на поведенческих характеристиках человека. Это особенности, которые характерны для подсознательных движений в процессе каких-либо действий (речи, подписи, походки и т.д.). В качестве источника информации для идентификации личности отпечатки пальцев человека несут особый интерес в связи с уникальностью индивидуальных признаков. Вероятность отказа в доступе пользователям, уполномоченным для прохода, составляет меньше 0,000001 %. Есть два алгоритма, лежащих в основе распознавания отпечатков: по рельефу всей поверхности пальца и по отдельным деталям (или по характерным точкам), а также комбинирование данных алгоритмов. В СКУД, использующих дактилоскопию, применяются алгоритмические решения, которые позволяют отличить живой палец от мертвого или от муляжа. Достигается это определением температуры прикладываемого пальца, отслеживанием динамики потоотделения на поверхности кожи пальца и характера деформации изображения папиллярных линий на сканере.

Для идентификации индивидуальных данных в современных электронных СКУД ЯО используются устройства нескольких типов. Наиболее распространенными являются:

- кодонаборные устройства ПИН-кода (кнопочные клавиатуры);
- считыватели электронных карт;

– считыватели ключа «тач-мемори»;

– биометрические считыватели.

На сегодняшний день наибольшую популярность среди эксплуатирующих организаций получили различные варианты считывателей карт. Они имеют явное преимущество и удобство в использовании, однако при этом в автоматизированном пункте доступа контролируется «проход карточки, а не человека». Кроме того, существует вероятность потери карты или ее кражи злоумышленниками. Все эти факторы снижают возможность использования СКУД, основанных только на считывателях карт, в приложениях с высокими требованиями к уровню безопасности. Наиболее высокий уровень безопасности обеспечивают различные биометрические устройства контроля доступа, которые используют в роли идентификатора биометрические параметры человека (отпечатки пальцев, геометрия рук, рисунок сетчатки глаза и т. п.), однозначно предоставляющие доступ только определенному человеку – носителю кода (биометрических параметров).

Бесконтактные считыватели *HID Corporation*предназначаются для считывания информации с proximity-карты (пропуска) и последующей передачи ее в контроллер СКУД. Считыватель распознает персональный код, и на основе поступившей информации контроллер принимает решение о разрешении прохода или о его запрете для владельца пропуска в помещение, где на входе установлен считыватель. Вся процедура считывания информации с идентификатора занимает около одной миллисекунды.

Проксимити-считыватели с клавиатурой *ProxPro*используются в СКУД, к которым предъявляются повышенные требования по безопасности. Кроме считывателя карт, данные устройства имеют кодонаборную клавиатуру, предназначенную для ввода второго идентификационного признака (цифрового кода). Для системы характерны простота монтажа и надежность клавиатуры. При попытке несанкционированного вскрытия корпуса считывателя с клавиатурой срабатывает специальный встроенный датчик, который активирует сигнализацию.

Кодонаборные устройства–принцип работы данного типа устройств достаточно прост: если набранный на клавиатуре код доступа верен, то система позволяет пройти на охраняемую территорию. Носителем ПИН-кода будет являться память человека, поэтому следует рассматривать возможность ввода ПИН-кода пользователем под угрозой жизни ему, либо его близким. Для этого пользователь СКУД снабжается «кодом под принуждением» (как правило, это дополнительная цифра, вводимая после основного кода), при использовании которого доступ предоставляется, однако при этом на пост охраны подается сигнал тревоги. Расширенные возможности предоставляют электронные кодонаборные устройства, использующие для отображения информации светодиодные индикаторы. В этом случае для защиты от подсматривания вводимого кода применяются поляризационные фильтры, ограничивающие угол обзора, при котором можно различить отображаемые на клавиатуре цифры. Также используется эффект скремблирования (смешивания) – при каждом новом использовании клавиатуры цифры будут располагаться в случайном порядке.

На сегодняшний день использование систем биометрической идентификации приобретает все больший масштаб. СФЗ постоянно совершенствуется – тем самым повышается ее эффективность. Кроме того, согласно принципу адаптивности, СФЗ должна быть дополнена необходимыми изменениями (в связи с появлением новой модели нарушителя, изменением категории помещения и пр.). Поэтому чрезвычайно важен вопрос интеграции подсистемы биометрической идентификации в общую инфраструктуру СКУД объекта любого класса.

Для моделирования данной задачи была поставлена задача по созданию учебной интегрированной системы контроля и управления доступом на основе устройств биометрической идентификации «*BioSmart*» и СОЭН «Интеллкт».

2 Построение системы безопасности с применением устройств биометрической идентификации «BioSmart».

2.1 Назначение СКУД «BioSmart»

Руководствуясь требованиямик построению СФЗ, была созданаинтегрированная система контроля и управления доступом на основе биометрической системы «*BioSmart»*

СКУД «*BioSmart»* является сетевой, распределенной системой, с разграничением прав доступа пользователей, при необходимости наращиваемой, открытой для интеграции с оборудованием других производителей. В точках прохода устанавливаются контроллеры, подключаемые к управляющему ПК или серверу по интерфейсу *RS*485 или локальной сети *Ethernet*. Магистраль *RS*485 организуется при помощи преобразователей (*USB-RS*485, *LAN-RS*485, *GPRS-RS*485).

СКУД «*BioSmart»* выполняет следующие функции[13]:

- идентификация человека путем сканирования отпечатка пальца;
- доступ только зарегистрированных сотрудников и посетителей;
- управление исполнительными устройствами (дверями, турникетами, шлагбаумами);
- формирование сигнала тревоги при попытке несанкционированного доступа;
- ведение журнала событий;
- разграничение доступа по временным зонам;
- мониторинг событий в реальном времени;
- возможность доступа в режимах: отпечаток или карта, карта и отпечаток.

Интеграция биометрических контроллеров с существующими системами безопасности позволяет повысить надежность и уменьшить вероятность проникновения злоумышленников и утечки информации. Для интеграции с устройствами сторонних производителей на

плате контроллера «*BioSmart*» присутствует вход и выход интерфейса *Wiegand* работающего в диапазоне от 26 до 40 бит. Выход интерфейса *Wiegand* позволяет интегрировать контроллер «*BioSmart*» в любую СКУД. В случае успешной идентификации по отпечатку пальца, контроллер «*Biosmart»* передает код аналогичный коду карты на контроллер сторонней СКУД. В свою очередь, контроллер СКУД принимает решение о допуске и подаёт сигнал на исполнительное устройство. При таком подходе значительно снижаются расходы на модернизацию существующей карточной системы на биометрическую, достаточно заменить только считыватели, а контроллер, база данных сотрудников, исполнительные устройства и кабельные трассы остаются прежними. Вход интерфейса *Wiegand* позволяет подключать к контроллеру «*BioSmart»* считыватель проксимити карт или кодонаборную панель. Такой режим может использоваться для двухфакторной идентификации в режимных помещениях или для организации режима шлюза, т.е. сначала пользователю необходимо приложить карту либо ввести пароль, потом приложить палец к контроллеру«*BioSmart*». Самым распространенным решением является организация гостевого доступа на предприятие по карточкам, а сотрудники предприятия проходят по отпечаткам. Также существует возможность интеграции с охранной сигнализацией, для постановки или снятия помещения с охраны.

2.2 Формирование требований к учебной системе

Предлагаемая система позволяет моделировать пропускной режим, реально существующий на ЯО с применением индивидуальных биометрических характеристик человека. За основу принимались требования, изложенные ранее в пункте 1.3.2. Адаптированные требования для данной учебной системы и особенности ее реализации представлены ниже более подробно.

Разрабатываемая система контроля и управления доступом строится на основе СКУД BioSmart и предназначена для наглядного представления, формирования и реализации процедур обеспечения санкционированного доступа.При этом также имеется возможность устанавливать разграничение прав доступа персонала (посетителей, командированных лиц) в помещения объекта, а также несанкционированного доступа нарушителей в охраняемые помещения. В случае обнаружения попыток несанкционированного доступа, а также при выявлении фактов силового воздействия на элементы конструкций пропускных устройств, соответствующая информация в реальном масштабе времени предоставляться на пункт охраны.

В системе разрабатывается протоколирование и архивирование всех совершаемых действий, в том числе в автономных режимах работы системы и считывателей BioSmart.

Обоснование выбора системы BioSmart заключается в следующем.Был проведен анализ рынка оборудования биометрических систем доступа, и была выбрана российская биометрическая СКУД BioSmart, как состоящая из широкого спектра оборудования и позволяющая организовать эффективную, надежную и экономичную систему контроля и управления доступом. СКУД BioSmart позволяет создавать системы управления доступом любого масштаба и сложности: от локальных (на одну точку доступа) до сетевых систем, рассчитанных на крупные территориально-распределенные объекты.

Выбранная биометрическая система отвечает всем современным требованиям, предъявляемым к таким системам. Она обеспечивает высокий уровень защищенности личных данных сотрудников, обеспечение контроля посещаемости и трудовой дисциплиной, интеграцию с любыми существующими СКУД и интегрированными системами безопасности.

2.3 Принцип работы системы «BioSmart»

Методика биометрической аутентификации заключается в следующем. При обращении с запросом к СКУД на доступ, прежде всего, пользователь идентифицирует себя с помощью карточки, ключа или личного идентификационного номера. Система сверяет предъявленный пользователем идентификатор с личным файлом (эталоном) пользователя в своей памяти, где вместе с номером хранятся данные его биометрии, которые предварительно были зафиксированы во время процедуры регистрации пользователя. После этого сотрудник предъявляет системе для считывания носитель биометрических параметров. Сравнивпоступившие и зарегистрированные данные, система предоставляет или запрещает доступ. Таким образом, наряду с измерителями биометрических характеристик СКУД должны быть оборудованы соответствующими считывателями идентификационных карточек или пластиковых ключей (или цифровой клавиатурой).

Для идентификации личности по узору папиллярных линий пальца сотрудникпомещает палец на окно сканирующего устройства. При совпадении получаемых признаков с эталонными, которые предварительно заложены в память ЭВМ, подается команда исполнительному устройству. Хотя рисунок капиллярных линий пальцев индивидуален, использование полного набора их признаков чрезмерно усложняет устройство идентификации. Поэтому с целью его удешевления применяют признаки, наиболее легко измеряемые автоматом. Выпускают сравнительно недорогие устройства идентификации по отпечаткам пальцев, действие которых

основано на измерении расстояния между основными дактилоскопическими признаками. Процесс аутентификации по отпечаткам пальцев показан на рисунке 4.

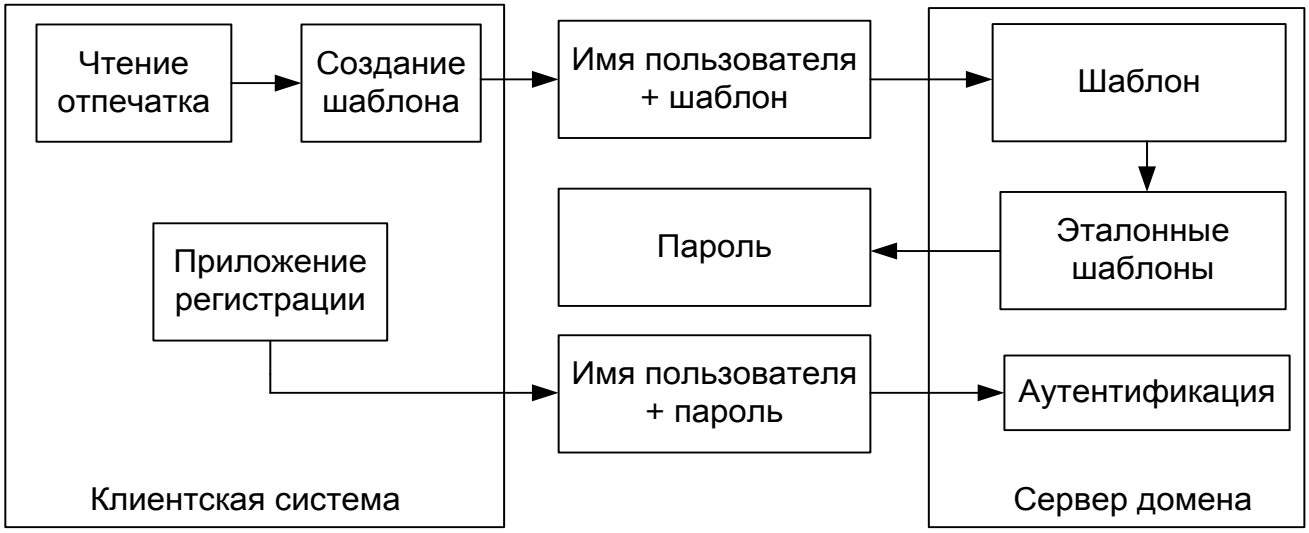

Рисунок 4 – Процесс аутентификации по отпечаткам пальцев

Дактилоскопия построена на двух основных качествах, присущих папиллярным узорам кожи пальцев и ладоней:

– стабильность рисунка узора на протяжении всей жизни человека;

– уникальность рисунка, означающее отсутствие двух индивидуумов с одинаковыми дактилоскопическими отпечатками.

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), местоположение которых задается в декартовой системе координат. Регистрация пользователей производится в программе BioSmart-Studio. Регистрации отпечатков пальцев может быть произведена как при помощи контрольного считывателя, подключаемого через USB порт персонального компьютера, так и при помощи сканера, находящемся непосредственно на контроллере «BioSmart», либо на биометрическом терминале BioSmart WTC. На каждого пользователя можно зарегистрировать до пяти отпечатков пальцев и один код бесконтактной карты формата EmMarine, Mifare или HID. В базу данных СКУД «BioSmart» записываются математические шаблоны

отпечатков, что делает невозможным обратное воссоздание их графического изображения. Далее, пользователю присваиваются права доступа на конкретные точки прохода, информация о пользователе передается на контроллер «BioSmart» или сервер идентификации в защищенном виде. Когдапользователь прикладывает палец или пластиковую карту к сканеру, происходит поиск в базе данных зарегистрированных шаблонов. В режиме серверной идентификации, поиск и сравнение шаблонов происходит на внешнем сервере, что увеличивает скорость обработки больших баз данных. При успешной идентификации контроллер «BioSmart» генерирует управляющий сигнал на исполнительные устройства (электромагнитный замок, турникет и пр.) непосредственно, либо через блок управления реле (БУР). БУР устанавливается внутри помещения, что исключает возможность несанкционированного доступа в помещение путем замыкания проводов или имитации сигнала управления. При успешной идентификации в журнал событий записывается соответствующая информация, используемая в дальнейшем для учета рабочего времени и генерации различных отчетов. Существует возможность вывода всех событий в реальном времени в режиме мониторинга. События неуспешной идентификации или попытки несанкционированного доступа пользователей фиксируются в системе.

2.4Структурная схема СКУД BioSmart

СКУД BioSmart является сетевой системой, с разграничением прав доступа пользователей, при необходимости наращиваемой, открытой для интеграции с устройствами других производителей.

Структурная схема учебной системы представлена на рисунке 5.

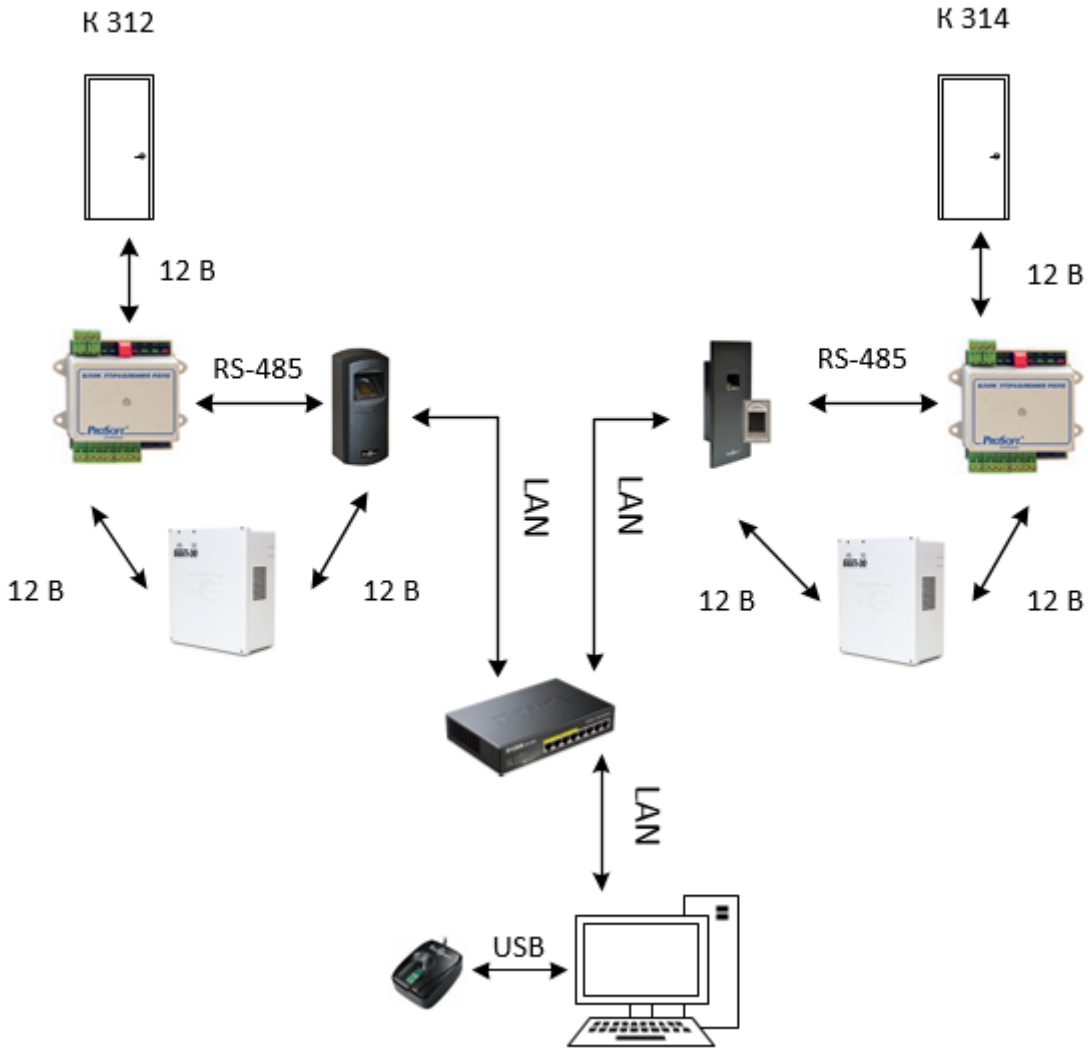

Рисунок 5 – Структурная схема учебной системы

Регистрация пользователей производится с помощью ПО BioSmart-Studio и контрольного считывателя, подключаемого через USB-порт персонального компьютера. На каждого пользователя можно зарегистрировать до 10 отпечатков пальцев. При этом в базу данных записываются математические шаблоны отпечатков, что делает невозможным обратное воссоздание их графического изображения. Далее пользователю присваиваются права доступа на конкретные точки прохода, при этом шаблоны отпечатков в кодированном виде передаются по линии связи в контроллер BioSmart.

Когда пользователь прикладывает палец к сканеру контроллера BioSmart, происходит поиск в базе данных контроллера зарегистрированных шаблонов. При успешной идентификации контроллер выдает управляющий сигнал на блок управления реле по защищенному цифровому каналу, который в свою очередь включает исполнительные устройства (электромагнитные замки, турникеты и пр.). Тем самым исключается возможность несанкционированного доступа в помещение путем перемыкания проводов или имитации сигнала управления. При успешной идентификации в журнал событий записывается соответствующая информация. В случае неуспешной идентификации фиксируется событие об отказе доступа.

Контроллер BioSmart может работать с внешними датчиками, для этого на блоке управления реле предусмотрены два дискретных входа. Первый дискретный вход применяется для подключения выносной кнопки выхода из помещения. Второй дискретный вход может применяться для подключения датчика пожарной сигнализации. В случае пожара и срабатывания датчика, защита с точек прохода снимается. Все события по внешним датчикам также фиксируются в журнале.

СКУД BioSmart имеет возможность интеграции с системами контроля доступа сторонних производителей по интерфейсу Wiegand-26. Таким образом, есть возможность модернизации уже установленной системы контроля доступа по пластиковым картам на биометрическую. Либо можно существенно повысить уровень безопасности на предприятии, путем использования двухуровневой идентификации (электронная карточка + отпечаток).

Если на предприятии не установлена система контроля доступа по карточкам, а требуется использование двухуровневой идентификации для повышения уровня безопасности, в СКУД BioSmart предусмотрена возможность подключения стандартного считывателя пластиковых карт по интерфейсу Wiegand-26. При этом будет возможна организация пропускного

режима, как по карте, так и по отпечатку, а также совместный режим работы (сначала необходимо приложить карточку к proximity-считывателю, потом палец к биометрическому считывателю).

Имеющаяся возможность подключения стандартного считывателя пластиковых карт так же позволяет более эффективно организовать систему «гостевого входа» для предприятий с большим количеством посетителей в день. Использование «гостевых карт» позволяет существенно упростить процедуру регистрации гостя и исключить влияние человеческого фактора, т.к. в системе можно заранее указать все права доступа на точки прохода для «гостевых карт».

2.5Основные компоненты и программное обеспечение СКУД

Рассмотрим подробное описание выбранных устройств биометрической системы.

Контроллер биометрический BioSmart (накладной) (рисунок 6) предназначен для идентификации пользователей по отпечаткам пальцев, бесконтактным пластиковым картам и управления устройствами доступа (замок, турникет).

Рисунок 6 – Контроллер биометрический BioSmart (накладной)

Контроллер имеет энергонезависимую память на 9000 отпечатков пальцев и 12800 событий. Все события в контроллере записываются в хронологическом порядке с указанием точного времени прохода сотрудников. Контроллер оснащен световым индикатором и звуковым зуммером для информирования пользователя о результатах идентификации.

Особенности данного устройства:

– встроенный считыватель пластиковых карт стандарта EM-Marine;

– контроллер с емкостным сканером (SteelCoat) обеспечивает надежную защиту от муляжей отпечатков пальцев и незначительных механических повреждений;

– контроллер с оптическим сканером обеспечивает надежную защиту от механических повреждений (царапины, сколы и т.д.).

Контроллер биометрический BioSmart во врезном исполнении (рисунок 7) предназначен для идентификации пользователей по отпечаткам пальцев, бесконтактным пластиковым картам и управления устройствами доступа (замок, турникет).

Рисунок 7 – Контроллер биометрический BioSmart (врезной)

Контроллер имеет энергонезависимую память на 500 отпечатков пальцев, 40000 событий. Все события в контроллере записываются в

хронологическом порядке с указанием точного времени. Контроллер оснащен световым индикатором и звуковым зуммером для информирования пользователя о результатах идентификации.

Особенности идентичны с накладным контроллером:

– контроллер с емкостным сканером (SteelCoat) обеспечивает надежную защиту от муляжей отпечатков пальцев и незначительных механических повреждений;

– контроллер с оптическим сканером обеспечивает надежную защиту от механических повреждений (царапины, сколы и т.д.);

– контроллер оснащен световым индикатором и звуковым зуммером для информирования пользователя о результатах идентификации;

– врезная конструкция способствует защищенности внутренних частей контроллера.

Для считывания отпечатков пальцев и внесения их в базу данных используется сканер отпечатков пальцев для ПК FS-80.Он представляет собой модуль для захвата и передачи на ПК образа отпечатка пальца. (рисунок 8) Уникальная технология, использующая прецизионную CMOS матрицу, позволяет получать изображения отпечатка пальца с высоким качеством. Сканер FS-80 может применяться в любых приложениях, где требуется эффективная и достоверная идентификация человека. В сканер FS-80 встроена специальная электронная схема – LFD, позволяющая отличить живой палец от муляжа.

Рисунок 8 – Сканер отпечатков пальцев для ПК FS-80

Для управления исполнительными устройствами (замки, турникеты, шлагбаумы) используется Блок управления реле BioSmart (рисунок 9). Он обеспечивает работу с внешними датчиками охранно-пожарных сигнализаций и управляется командами с контроллера BioSmart через линию связи RS485. К БУР BioSmart можно подключить до 4-х контроллеров.

Рисунок 9 – Блок управления реле BioSmart

Программное обеспечение BioSmart-Studio позволяет управлять базой данных отпечатков пальцев пользователей, формировать отчеты, управлять группами считывателей, а также назначать временные зоны доступа сотрудников. Система поддерживает платформы Microsoft Access и SQL Server. ПО может работать по «клиент - серверной» технологии и удаленно подключаться к базе данных в сети Ethernet.

Основные функции, выполняемые ПО BioSmart-Studio следующие:

– регистрация сотрудников или групп сотрудников в системе и управление базой данных позволять заносить персональные данные сотрудников, отпечатки пальцев, фотографии и любую необходимую дополнительную информацию;

– ведение базы данных сотрудников (электронная картотека) дает возможность обращения к информации в любое время;

– назначение прав доступа дает возможность создать различные категории доступа сотрудников;

– назначение повременного доступа запрещает проход в выходные и праздничные дни, позволяет вести рабочий график и контролировать опоздания;

– мониторинг событий и формирование журнала событий позволяет вести контроль в реальном режиме времени и дает возможность обращения к архивам;

– конфигурирование и настройка системы позволяет адаптировать ее под особенности предприятия;

– управление исполнительными механизмами в режиме мониторинга дает возможность ручного управления системой в реальном режиме времени.

Biosmart-Studio имеет широкие возможности по генерации и настройке необходимых отчетов (статистика доступа к объектам, статистика проходов/передвижения сотрудников, табель учета рабочего времени с различной степенью детализации, отчет по нарушениям и нарушителям рабочего графика и пр.). Кроме того, возможно создание отчетов как по конкретному сотруднику или объекту, так и по группе сотрудников или объектов за указанный период времени.

Гибкая система экспорта/импорта позволяет обмениваться данными с другим ПО административного учета. Все виды отчетов могут быть легко экспортированы в программу Microsoft Excel для последующей обработки [21].

2.6 Настройка ПО BioSmartStudio.

При запуске программы BioSmart-Studio, на экране появится окно входа в программу (рисунок 9).

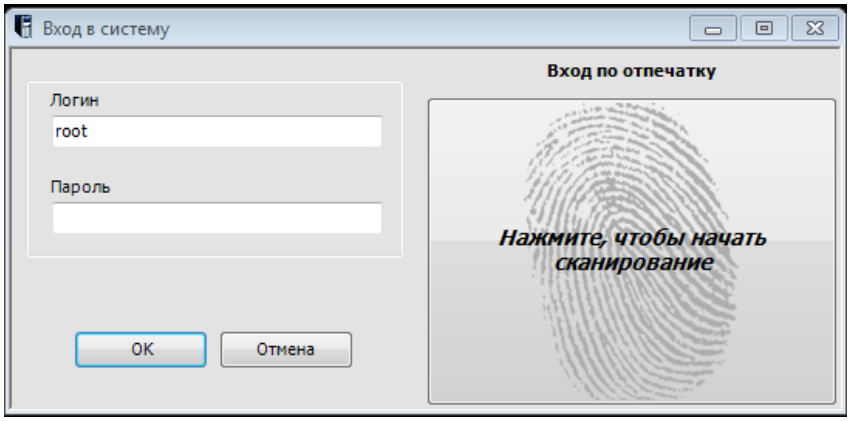

Рисунок 9 – Окно входа в программу

Для входа в программу при первом запуске достаточно нажать кнопку «ОК». В последствии, для входа в программу в поле «Логин» необходимо ввести имя пользователя, выполняющего вход в программу. Кроме того, для авторизации пользователя необходимо ввести пароль или приложить отпечаток. В зависимости от типа аутентификации, назначенного данному пользователю администратором системы. Права администратора системы имеет учетная запись «root».

После идентификации пользователя появляется главное окно программы (рисунок 10).

В левой части окна расположен ряд раскрывающихся панелей, количество и содержание которых зависит от контекста и настроек «вида» окна. Отображение панелей можно отключить, сняв галочку в соответствующем пункте меню Вид–Панели[15].

– «Информация» – отображает информацию о количестве объектов обозреваемой категории;

– «Действия» – содержит список возможных действий для объектов обозреваемой категории;

– «Фильтры» – содержит набор инструментов для фильтрации списка обозреваемых объектов по определенному критерию (доступна для объектов «сотрудники» и «журналы»);

– «Дерево элементов» – содержит дерево доступных компонентов (категорий объектов) для быстрой навигации.Правая часть окна изначально содержит список доступных пользователю функциональных компонентов.

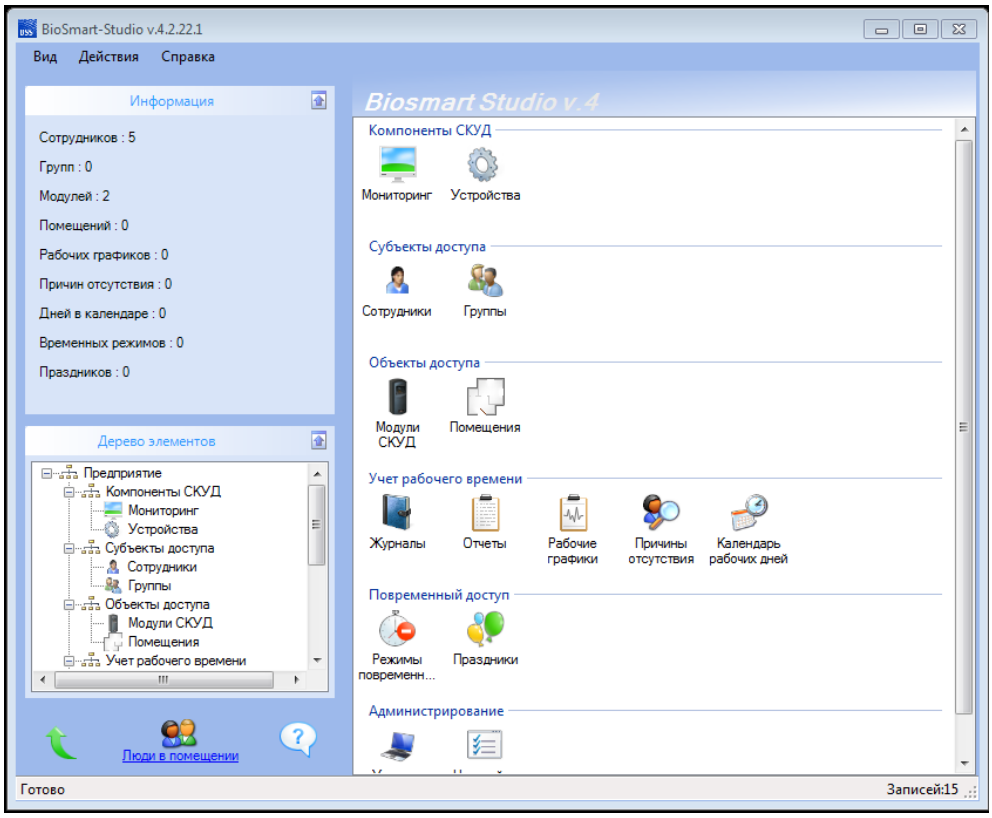

Рисунок 10 – Главное окно программы

Состав этого списка и характер доступа определяется для каждого пользователя администратором программы, исходя из функциональных обязанностей пользователя.

После входа в программу был выполнен поиск модулей системы. Для организации связи программы с модулями BioSmart используется Ethernet или USB- преобразователи интерфейса. Чтобы сообщить программе об их существовании в системе, следует воспользоваться панелью «Настройки ПО». После регистрации существующих конвертеров в системе, необходимо произвести поиск модулей BioSmart через компонент «Устройства». Последовательный поиск модулей BioSmart позволяет серверу контроллеров сформировать таблицу маршрутизации модулей (т.е. набор пар <модуль BioSmart, конвертер>), а также обновить прошивку модулей (рисунок 11).

Следует отметить, что разработанная система не содержит в себе конвертеров, а соединение с модулями проходит через Ethernetсоединение. Таким образом поиск модулей в системе проходит путем сканирования сети на предмет сетевых карт модулей. Важно учитывать, чтобы фаерволл на маршрутизаторе, через который происходит соединение, был выключен, в противном случае поиск модулей системы станет невозможным.

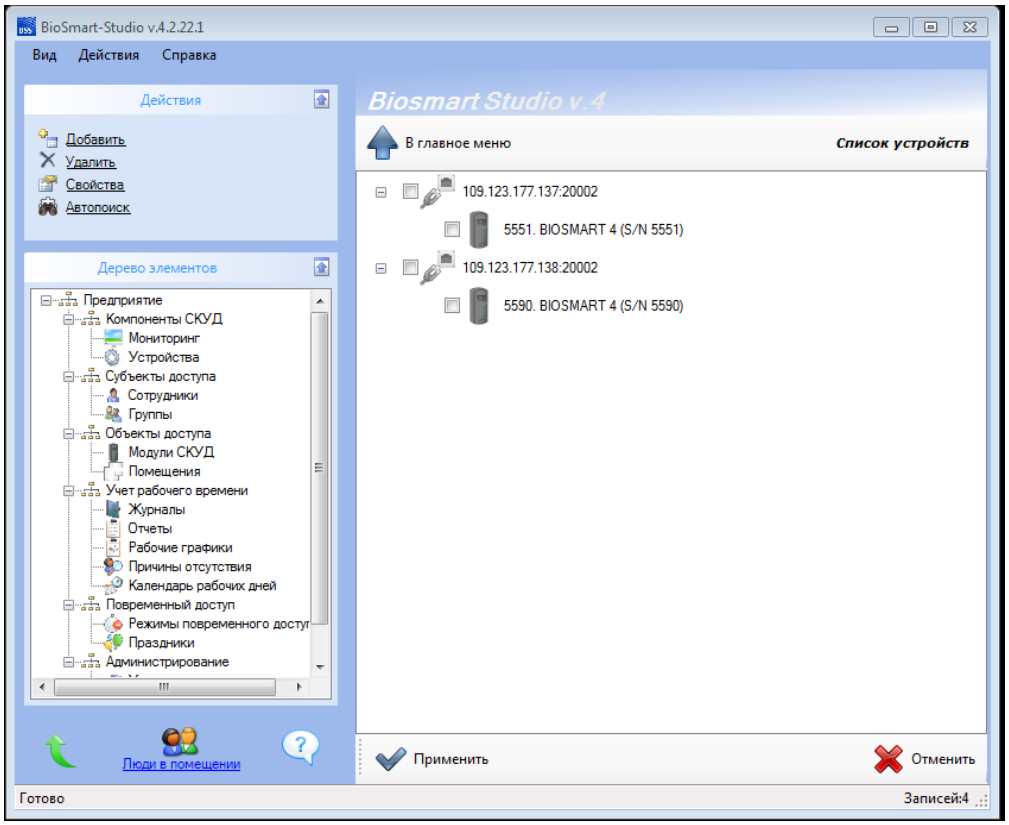

Рисунок 11 – Окно компонентов СКУД

Следует учесть, что добавление устройства не означает регистрацию модуля BioSmart в базе данных. Для полноценной работы программы с модулем (регистрация отпечатков, обновление журналов и т.д.), необходимо добавить модуль BioSmart через группу объектов «Модули СКУД».

После успешного поиска модуля СКУД была выполнена его настройка, и настройка БУРа, этого модуля, в зависимости от его назначения. При настройке БУРа, необходимо, выбрать действия при срабатывании реле. При настройке модуля BioSmart можно выбрать вариант его срабатывания. Так как в разрабатываемой учебной системе присутствует модуль с

интегрированным считывателем магнитных карт, можно настроить двойную идентификацию. Реализуется это путем выполнения сценария, при котором, идентифицируемому пользователю необходимо сначала приложить свою уникальную карту, затем приложить палец для сканирования отпечатка пальца. В случае успешной идентификации, модуль учебной системы подаст сигнал на блок управления реле, после чего блок управления реле, разомкнет магнитный замок.Окно настройки модуля учебной системы представлено на рисунке 12.

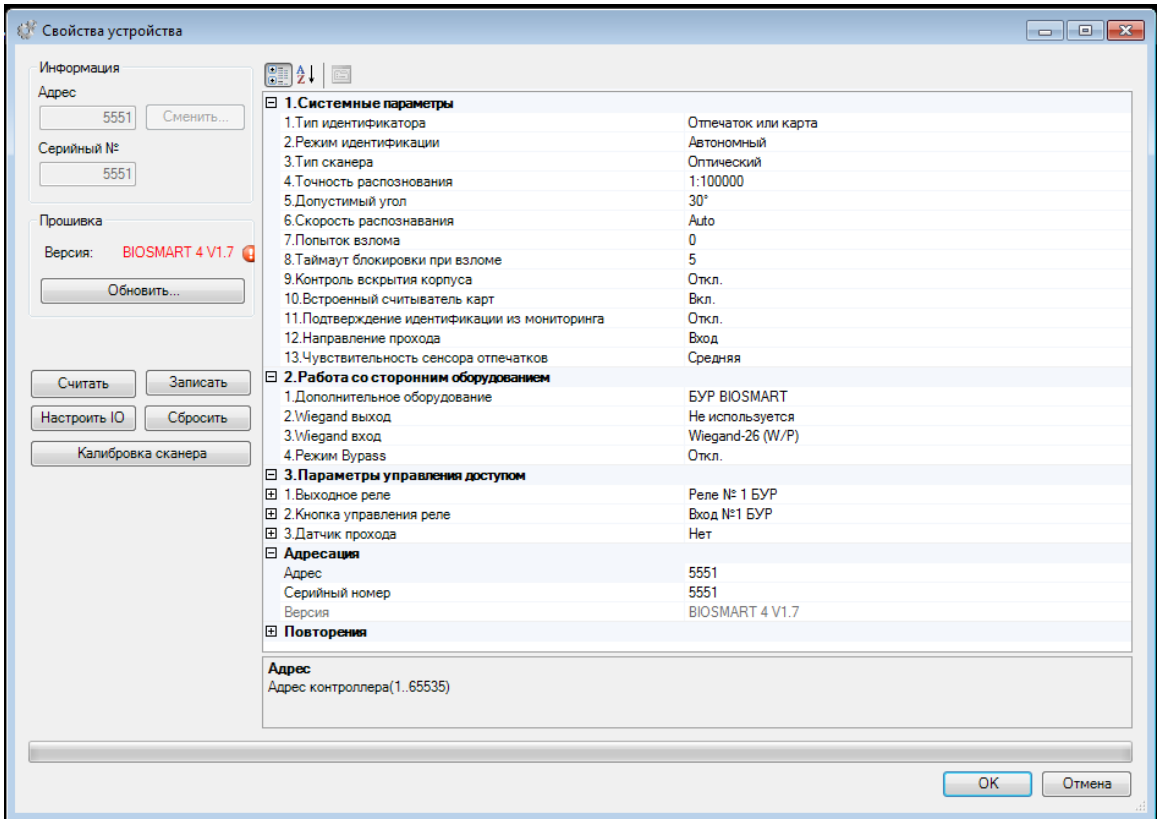

Рисунок 12 – Окно настройки модуля учебной системы

3 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

Целью данного раздела является проектирование и создание конкурентоспособных разработок и технологий, отвечающих предъявляемым требованиям в области ресурсоэффективности и ресурсосбережения.

Достижение цели обеспечивается решением задач:

- разработка общей экономической идеи проекта, формирование концепции проекта;
- организация работ по научно-исследовательскому проекту;
- определение возможных альтернатив проведения научных исследований;
- планирование научно-исследовательских работ;
- оценки коммерческого потенциала и перспективности проведения научных исследований с позиции ресурсоэффективности и ресурсосбережения;
- определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования.

В данной работе была разработана и создана интегрированная учебная система безопасности на основе средств «BioSmart»

3.1 Потенциальные потребители результатов работы

Результатом работы являетсяучебная система безопасности на основе средств биометрии.

Целевым рынком данного исследования будут являться режимные объекты, требующие повышенные меры безопасности на границах. К ним можно отнести объекты ядерно-топливного цикла.

Сегментировать рынок услуг можно по степени потребности использования данной системы безопасности. Результаты сегментирования представлены в рисунке 3.1.

		Атомная промышленность	Военная промышленности	Научные – исследовательские институты
Потребность	Сильная			
	Слабая			

Рисунок 3.1 – Карта сегментирования рынка услуг по использованию оптимальной методики измерения

3.1.1 Анализ конкурентных технических решений

Контроль доступа на базе считывателей биометрических параметров может решать одновременно две противоположные задачи: повышение уровня комфорта, повышение уровня безопасности наиболее охраняемых мест на объекте. При этом безопасность обеспечивается не каким-то одним элементом системы, а комплексом организационных мер и технических средств СФЗ. Конкурентами являются:

- Средства контроля доступа на основе Proximityкарт;
- Средства контроля доступа на основе код-пароелй.

Оценочная карта анализа представлена в таблице 3.1.1. Позиция разработки и конкурентов оценивается по каждому показателю экспертнымпутем по пятибалльной шкале, где 1 – наиболее слабая позиция, а 5 – наиболее сильная. Веса показателей, определяемые экспертным путем, в сумме должны составлять 1.Анализ конкурентных технических решений определяется по формуле:

$$K = \sum B_i \cdot Б_i , \quad (1)$$

где K – конкурентоспособность научной разработки или конкурента;

B_i – вес показателя (в долях единицы);

$Б_i$ – балл i-го показателя.

Таблица 3.1.1 – Оценочная карта для сравнения конкурентных технических решений (разработок)

Критерии оценки	Вес критерия	Баллы			Конкурентоспособность		
		$Б_ф$	$Б_{к1}$	$Б_{к2}$	$К_ф$	$К_{к1}$	$К_{к2}$
1	2	3	4	5	6	7	8
Технические критерии оценки ресурсоэффективности							
1. Соответствие нормативным документам	0,1	5	4	3	0,5	0,4	0,3
2. Удобство эксплуатации	0,15	5	4	3	0,75	0,6	0,45
3. Автономность	0,03	5	2	3	0,15	0,06	0,09
4. Надежность	0,1	5	4	3	0,5	0,4	0,3
5. Возможность модернизации	0,05	5	5	5	0,25	0,25	0,25
6. Возможность интеграции	0,05	5	1	4	0,25	0,05	0,2
7. Стабильность	0,06	5	3	3	0,3	0,18	0,18
8. Доступность	0,1	5	4	4	0,5	0,4	0,4
Экономические критерии оценки эффективности							
1.Конкурентоспособность разрабатываемой системы	0,04	5	4	3	0,2	0,16	0,12
2. Стоимость разработки	0,12	5	1	3	0,6	0,12	0,36
3. Предполагаемый срок эксплуатации	0,1	5	2	3	0,5	0,2	0,3
4. Финансирование разработанного метода	0,1	5	1	3	0,5	0,1	0,3
Итого	1				5	2,92	3,25

На основании представленного выше анализа можно сделать вывод, что разработанная в данной работе модель является наиболее оптимальной для использования в практических целях. Конкурентные методы имеют ряд недостатков, исключаемых разработанной моделью. В свою очередь разработанная модель позволяет существенно снизить финансовые затраты, обеспечивает высокую точность расчётных значений и имеет высокий потенциал развития в дальнейшем.

3.1.2 SWOT-анализ

SWOT – Strengths (сильные стороны), Weaknesses (слабые стороны), Opportunities (возможности) и Threats (угрозы) – представляет собой комплексный анализ научно-исследовательского проекта. SWOT-анализ применяют для исследования внешней и внутренней среды проекта.

Сильные стороны – это факторы, характеризующие конкурентоспособную сторону научно-исследовательского проекта. Сильные стороны свидетельствуют о том, что у проекта есть отличительное преимущество или особые ресурсы, являющиеся особенными с точки зрения конкуренции. Другими словами, сильные стороны – это ресурсы или возможности, которыми располагает руководство проекта и которые могут быть эффективно использованы для достижения поставленных целей.

Слабые стороны – это недостаток, упущение или ограниченность научно-исследовательского проекта, которые препятствуют достижению его целей. Это то, что плохо получается в рамках проекта или где он располагает недостаточными возможностями или ресурсами по сравнению с конкурентами.

Возможности включают в себя любую предпочтительную ситуацию в настоящем или будущем, возникающую в условиях окружающей среды проекта, например, тенденцию, изменение или предполагаемую потребность, которая поддерживает спрос на результаты проекта и позволяет руководству проекта улучшить свою конкурентную позицию.

Угроза представляет собой любую нежелательную ситуацию, тенденцию или изменение в условиях окружающей среды проекта, которые имеют разрушительный или угрожающий характер для его конкурентоспособности в настоящем или будущем.

В таблице 3.1.2 представлена интерактивная матрица проекта, в которой показано соотношение сильных сторон с возможностями, что позволяет более подробно рассмотреть перспективы разработки.

Таблица 3.2 – Интерактивная матрица проекта

Возможности проекта	Сильные стороны проекта				
	С1	С2	С3	С4	С5
В1	+	+	+	+	+
В2	+	+	+	+	+
В3	+	+	+	+	+
В4	+	+	+	+	+
В5	+	+	+	+	+

В матрице пересечения сильных сторон и возможностей имеет определенный результат: «плюс» – сильное соответствие сильной стороны и возможности, «минус» – слабое соотношение.

В результате была составлена итоговая матрица SWOT-анализа, представленная в таблице 3.1.3.

Таблица 3.2.1 – SWOT-анализ

	Сильные стороны проекта: С1. Актуальность выбранной темы. С2. Применение современного оборудования. С3. Возможность интеграции сторонних СКУД. С4. Возможность расширения системы. С5. Возможность автономной работы.	Слабые стороны проекта: Сл1. Относительно высокая стоимость. Сл2. Ограниченный круг потребителей. Сл3. Необходимость создания сервера для большого количества данных пользователей. Сл4. Ограниченное число пользователей при работе в автономном режиме
Возможности: В1. Использование учебной системы для выполнения лабораторных работ. В1 Интеграция в учебную систему сторонних программ. В3. Расширение учебной системы. В4. Модернизация учебной системы. В5. Подготовка кадров в сфере биометрических систем.	Результаты анализа интерактивной матрицы проекта полей «Сильные стороны и возможности»: 1. Полное обеспечение условий для создания кадров в области биометрических систем. 2. Появление дополнительного спроса и финансирования, обеспеченных актуальностью тематики. 3. Постоянная модернизация системы, что делает ее конкурентоспособной.	Результаты анализа интерактивной матрицы проекта полей «Слабые стороны и возможности»: 1. Необходимо финансирование на модернизацию, что возможно реализовать в условиях вуза. 2. Расширение круга потребителей путем модернизации системы.

Продолжение таблицы 3.2.1

Угрозы: У1. Низкий спрос со стороны заказчиков. У2. Вероятность разработки подобных системдругими организациями. У3. Упразднение специальности, где может изучаться данная система У4. Отсутствие лицензии на применение системы в атомной-промышленности. У5. Разработка новейших СКУД	Результаты анализа интерактивной матрицы проекта полей «Сильные стороны и угрозы»: 1. Благодаря возможностям системы своевременному финансированию продвижение на рынок может стать успешным. 2. Так как существует возможность модернизации и интеграции системы, то это позволит конкурировать с новейшими разработками. .	Результаты анализа интерактивной матрицы проекта полей «Слабые стороны и угрозы»: 1. Относительно высокая стоимость, и ограниченный круг потребителей может вызвать низкий спрос со стороны заказчиков

Таким образом, выполнив SWOT-анализ можно сделать вывод, что на данный момент преимущества разработанной учебной системы значительно преобладают над её недостатками. Все имеющиеся несовершенства можно легко устранить, воспользовавшись перечисленными выше возможностями.

3.3 Планирование управления научно-техническим проектом

3.3.1 Контрольные события проекта

Ключевые события работы, их даты и результаты приведены в таблице 3.2.1.

Таблица 3.3.1 – Контрольные события проекта

№	Контрольное событие	Дата	Результат (подтверждающий документ)
1	Разработка технического задания на НИР	1.02.2017	Приказ по ФТИ
2	Составление и утверждение технического задания	3.02.2017	Задание на выполнение исследования
3	Выбор направления исследований	5.02.2017	
4	Подбор и изучение материалов по теме	10.02.2017	Отчёт
5	Календарное планирование работ	12.02.2017	План работ
6	Изучение возможностей учебной системы	13.02.2017	Отчёт

Продолжение таблицы 3.3.1

7	Монтаж учебной системы	14.02.2017	Отчёт
8	Настройка учебной системы	15.02.2017-30.03.2017	Отчёт
9	Составление методики работы с системой	28.03.2017	Отчёт
10	Обобщение и оценка результатов	30.03.2017	Отчёт
11	Составление пояснительной записки	14.02.2017-25.04.2017	Пояснительная записка
12	Проверка правильности выполнения ГОСТа пояснительной записки	26.04.2017	
13	Подготовка к защите	27.04.2017-25.05.2017	

3.2.2 План проекта

В рамках планирования учебной системы построен календарный план-график с помощью диаграммы Ганта. В данном случае работы по теме представляются протяженными во времени отрезками, характеризующимися датами начала и окончания выполнения работ.

Линейный график представлен в таблице 3.2.3.

Таблица 3.2.2 – Календарный план проекта

Код работы	Название	Длительность, дни	Дата начала работ	Дата окончания работ	Состав участников
1	Разработка технического задания	2	1.02.2017	3.02.2017	Руководитель
2	Составление и утверждение технического задания	2	3.02.2017	5.02.2017	Руководитель
3	Выбор направления работы	5	5.02.2017	10.02.2017	Студент
4	Подбор и изучение материалов по теме	2	10.02.2017	12.02.2017	Студент
5	Календарное планирование работ	1	12.02.2017	13.02.2017	Руководитель, студент
6	Изучение возможностей учебной системы	1	13.02.2017	14.02.2017	Студент
7	Монтаж учебной системы	20	14.02.2017	06.03.2017	Студент
8	Настройка учебной системы	22	06.03.2017	28.03.2017	Студент
9	Составление методики работы с системой	3	28.03.2017	30.03.2017	Студент

Продолжение таблицы 3.2.2 Календарный план проекта

10	Обобщение и оценка результатов	1	30.03.2017	30.03.2017	Руководитель, студент
11	Составление пояснительной записки	72	14.02.2017	25.04.2017	Студент
12	Проверка правильности выполнения ГОСТа пояснительной записки	1	26.04.2017	27.04.2017	Руководитель, студент
13	Подготовка к защите	29	27.04.2017	25.05.2017	Студент

В таблице 3.2.4 представлен календарный план-график проведения научного исследования.

Таблица 3.2.4 – Календарный план-график проведения научного исследования

№ работ	Вид работ	Исполнители	$T_к$, кал.дн.	Продолжительность выполнения работ													
				Февраль			Март			Апрель			Май			Июнь	
				1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	Разработка технического задания	Руководитель	2														
2	Составление и утверждение технического задания	Руководитель	2														
3	Выбор направления работы	Руководитель, студент	5														
4	Подбор и изучение материалов по теме	Студент	2														
5	Календарное планирование работ	Руководитель, студент	1														
6	Изучение возможностей учебной системы	Студент	1														
7	Монтаж учебной системы	Студент	20														
8	Настройка учебной системы	Студент	22														
9	Составление методики работы с системой	Студент	3														
10	Обобщение и оценка результатов	Руководитель, студент	1														
11	Составление пояснительной записки	Студент	72														
12	Проверка правильности выполнения ГОСТа пояснительной записки	Руководитель, студент	1														
13	Подготовка к защите	Студент	29														

− Руководитель − Студент

3.4 Бюджет научного исследования

При планировании бюджета исследования должно быть обеспечено полное и достоверное отражение всех видов расходов, связанных с его выполнением. В процессе формирования бюджета используется следующая группировка затрат по статьям:

- материальные затраты;
- затраты на специальное оборудование для научных (экспериментальных) работ;
- основная заработная плата исполнителей темы;
- дополнительная заработная плата исполнителей темы;
- отчисления во внебюджетные фонды (страховые отчисления);
- накладные расходы.

3.4.1 Расчёт материальных затрат

Расчет материальных затрат осуществляется по следующей формуле:

$$З_{\text{м}} = (1 + k_{\text{Т}}) \cdot \sum_{i=1}^{m} Ц_i \cdot N_{\text{расх}i},$$

где m – количество видов материальных ресурсов, потребляемых при выполнении научного исследования;

$N_{\text{расх}i}$ – количество материальных ресурсов i-го вида, планируемых к использованию при выполнении научного исследования (шт., кг, м, м^2 и т.д.);

$Ц_i$– цена приобретения единицы i-го вида потребляемых материальных ресурсов (руб./шт., руб./кг, руб./м, руб./м^2 и т.д.);

k_T– коэффициент, учитывающий транспортно-заготовительные расходы, принимаются в пределах 15 – 25 % от стоимости материалов.

Основными затратами в данной исследовательской работе являются затраты на электроэнергию и приобретение канцелярских товаров. Результаты расчётов по затратам на материалы приведены в таблице 3.3.1.

Затраты на электроэнергию рассчитываются по формуле:

$$C = Ц_{эл} \cdot P \cdot F_{об} = 2{,}17 \cdot 0{,}5 \cdot 960 = 984,$$

где $Ц_{эл}$ – тариф на электроэнергию (5,8 руб. за 1 кВт·ч);

P – мощность оборудования, кВт;

$F_{об}$ – время использования оборудования, ч.

Затраты на электроэнергию составили 984 рубля.

Таблица 3.4.1 – Материальные затраты

Наименование	Марка, размер	Количество	Цена за единицу, руб.	Сумма, руб.
Электроэнергия	–	480 кВт·ч	5.8	2784
Бумага	SvetoCopy	110	0,90	99
Печать на листе А4	–	110	1,5	165
Ручка	Pilot BPS-GP	1	50	50
Доступ в интернет	–	4 месяца	400	1600
Всего за материалы				2898
Транспортно-заготовительные расходы				0
Итого по статье $С_м$				7596

Данная статья включает в себя затраты на приобретение и организацию учебной системы безопасности. Определение затрат по этой статье производится по фактической стоимости с учётом транспортно-заготовительных расходов.

Таблица 3.4.1 – Оборудование для реализации учебной системы безопасности

№	Наименование изделия	Кол-во	Цена, руб.	Сумма, руб.
1	Контроллер биометрический «BioSmart»	2	19485	38970
2	Биометрический сканер для ПК	1	4890	4890
3	Программное обеспечение Biosmart-Studio	1	2980	2980
4	Компьютер(монитор, системный блок, мышь, клавиатура)	1	25600	25600
5	Электромагнитный замок	1	3384	3384

Продолжение таблицы 3.4.1 – Оборудование для реализации учебной системы безопасности

6	Кнопка разблокирования.	1	600	600
7	Блок бесперебойного питания, 317х302 х127 мм	2	2100	4200
8	Расходные материалы	1	3650	3650
9	Электронная карта HID	3	250	750
Итого: 85024 руб.				

3.4.2 Основная заработная плата исполнителей темы

Статья включает основную заработную плату работников, непосредственно занятых выполнением проекта, (включая премии, доплаты) и дополнительную заработную плату.

$$C_{зп} = З_{осн} + З_{доп},$$

где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата.

Основная заработная плата ($З_{осн}$) руководителя рассчитывается по следующей формуле:

$$З_{осн} = З_{дн} \cdot T_{раб},$$

где $З_{осн}$ – основная заработная плата одного работника;

$T_{раб}$ – продолжительность работ, выполняемых научно-техническим работником, раб.дн.

$З_{дн}$ – среднедневная заработная плата работника, руб.

Среднедневная заработная плата рассчитывается по формуле

$$З_{дн} = (З_{м} \cdot M) / F_{д},$$

где $З_{м}$ – месячный должностной оклад работника, руб.;

M – количество месяцев работы без отпуска в течение года:

- при отпуске в 24 раб. Дня М =11,2 месяца, 5-дневная неделя;
- при отпуске в 48 раб. дней М=10,4 месяца, 6-дневная неделя;

$F_{д}$ – действительный годовой фонд рабочего времени научно-технического персонала, раб. дн. (таблица 3.3.3).

Таблица 3.3.2 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Студент
Календарное число дней	365	365
Количество нерабочих дней: – выходные дни; – праздничные дни	 52 14	 104 14
Потери рабочего времени: – отпуск; – невыходы по болезни	 56 –	 48 –
Действительный годовой фонд рабочего времени	243	199

Студент во время прохождения преддипломной практики получает стипендию, равную 2275 руб/месяц. Среднедневная стипендия (оплата) составляет:

$$З_{дн} = (2275 \cdot 10,4) / 199 = 118,89 \text{руб/день.}$$

Основной заработок студента за время преддипломной практики составляет:

$$З_{осн} = 118,89 \cdot 84 = 9986,76 \text{ руб.}$$

Основная заработная плата научного руководителя рассчитывается на основании отраслевой оплаты труда. Отраслевая система оплаты труда в ТПУ предполагает следующий состав заработной платы:

– оклад – определяется предприятием. В ТПУ оклады распределены в соответствии с занимаемыми должностями, например, ассистент, ст. преподаватель, доцент, профессор.

– стимулирующие выплаты – устанавливаются руководителем подразделений за эффективный труд, выполнение дополнительных обязанностей и т.д.

– иные выплаты: районный коэффициент.

Руководителем данной научно-исследовательской работы является сотрудник с должностью доцент. Оклад доцентасоставляет 26300 рублей. Научный руководитель работает на 0,4 ставки. Районный коэффициент по Томску равен 1,3.

Основная заработная плата научного руководителя:

$$З_{м} = 26300 \cdot 0,4 \cdot 1,3 = 13676 \text{ руб / месяц.}$$

Среднедневная заработная плата научного руководителя:

$$З_{дн} = (13676 \cdot 10,4) / 243 = 574,05 руб / день.$$

3.4.3 Отчисления во внебюджетные фонды

Размер отчислений во внебюджетные фонды составляет 30 % от суммы затрат на оплату труда работников, непосредственно занятых выполнением исследовательской работы.

Величина отчислений во внебюджетные фонды определяется исходя из следующей формулы:

$$С_{внеб} = k_{внеб} \cdot (З_{осн} + З_{доп}),$$

где $k_{внеб}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования и пр.).

Величина отчислений во внебюджетные фонды составляет:

$$С_{внеб} = 0,3 \cdot 13676 = 4094,1 руб.$$

3.4.4 Накладные расходы

В эту статью включаются затраты на управление и хозяйственное обслуживание, которые могут быть отнесены непосредственно на конкретную тему. Кроме того, сюда относятся расходы по содержанию, эксплуатации и ремонту оборудования, производственного инструмента и инвентаря, зданий, сооружений и др.

Расчет накладных расходов ведется по следующей формуле:

$$С_{накл} = k_{накл} \cdot (З_{осн} + З_{доп}),$$

где $k_{накл}$ – коэффициент накладных расходов.

Накладные расходы в ТПУ составляют 12–16 % от суммы основной и дополнительной зарплаты работников, участвующих в выполнении темы. Примем $k_{накл}$ = 14 %.

Накладные расходы составляют:

$$С_{накл} = 0,14 \cdot (13676 + 9986,76) = 3312,78 руб.$$

3.4.5 Формирование бюджета затрат исследовательского проекта

Рассчитанная величина затрат научно-исследовательской работы является основой для формирования бюджета затрат проекта, который при формировании договора с заказчиком защищается научной организацией в качестве нижнего предела затрат на разработку научно-технической продукции.

Определение бюджета затрат на научно-исследовательский проект по каждому варианту исполнения приведен в таблице 3.3.6.

Таблица 3.3.6 – Расчёт бюджета затрат исследовательского проекта

Наименование статьи	Сумма, руб
1. Материальные затраты исследования	7596
3. Затраты по основной заработной плате исполнителей темы	23662,76
4. Отчисления во внебюджетные фонды	4722,32
5. Накладные расходы	3312,78
6. Затраты на оборудование	85024
Бюджет затрат работы	131913,86

3.5 Организационная структура проекта

Организационная структура проекта представляет собой временное структурное образование, создаваемое для достижения поставленных целей и задач проекта и включающее в себя всех участников процесса выполнения работ на каждом этапе.

Данной исследовательской работе соответствует функциональная структура организации. То есть организация рабочего процесса выстроена иерархически: у каждого участника проекта есть непосредственный руководитель, сотрудники разделены по областям специализации, каждой группой руководит компетентный специалист (функциональный руководитель).

Организационная структура научного проекта представлена на рисунке 3.4.

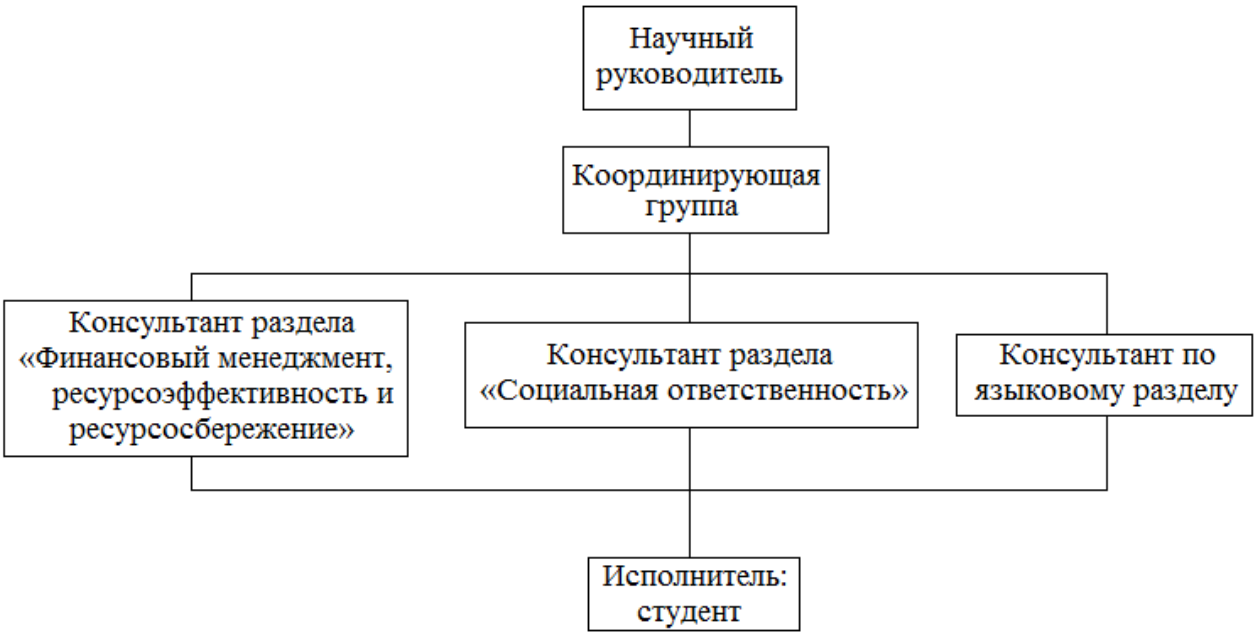

Рисунок 3.4 – Организационная структура научного проекта

3.6 Матрица ответственности

Степень ответственности каждого члена команды за принятые полномочия регламентируется матрицей ответственности. Матрица ответственности данного проекта представлена в таблице 3.5.

Таблица 3.5 – Матрица ответственности

Этапы проекта	Научный руководитель	Консультант раздела «Финансовый менеджмент»	Консультант раздела «Соцответственность»	Консультант по языковому разделу	Студент
Разработка технического задания	О				
Составление и утверждение технического задания	О				
Выбор направления работы	О				И
Подбор и изучение материалов по теме	С				И
Календарное планирование работ	О				И
Изучение возможностей учебной системы					И
Монтаж учебной системы					И
Настройка учебной системы	О				И
Составление методики работы с системой	О				И
Выполнение оценки ресурсоэффективности и ресурсосбережения		С			И
Выполнение раздела по социальной ответственности			С		И
Выполнение перевода части работы на английский язык				С	И
Обобщение и оценка результатов	С				И
Составление пояснительной записки	С				И
Проверка правильности выполнения ГОСТа пояснительной записки	С				И
Подготовка к защите	О				И

Степень участия в проекте характеризуется следующим образом:

– ответственный (О) – лицо, отвечающее за реализацию этапа проекта и контролирующее его ход;

– исполнитель (И) – лицо (лица), выполняющие работы в рамках этапа проекта.

– утверждающее лицо (У) – лицо, осуществляющее утверждение результатов этапа проекта (если этап предусматривает утверждение);

– согласующее лицо (С) – лицо, осуществляющее анализ результатов проекта и участвующее в принятии решения о соответствии результатов этапа требованиям.

3.7 Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования

Определение эффективности происходит на основе расчета интегрального показателя эффективности научного исследования. Его нахождение связано с определением двух средневзвешенных величин: финансовой эффективности и ресурсэффективности.

Интегральный показатель финансовой эффективности научного исследования получают в ходе оценки бюджета затрат трех (или более) вариантов исполнения научного исследования (см. табл. 3.6). Для этого наибольший интегральный показатель реализации технической задачи принимается за базу расчета (как знаменатель), с которым соотносится финансовые значения по всем вариантам исполнения.

Интегральный финансовый показатель разработки определяется:

$$I_{финр}^{испi} = \frac{Ф_{pi}}{Ф_{\max}},$$

где $I_{финр}^{испi}$ – интегральный финансовый показатель разработки;

$Ф_{pi}$ – стоимость i-го варианта исполнения;

$Ф_{\max}$ – максимальная стоимость исполнения научно-исследовательского проекта (в т.ч. аналоги).

Полученная величина интегрального финансового показателя разработки отражает соответствующее численное увеличение бюджета затрат разработки в разах (значение больше единицы), либо соответствующее численное удешевление стоимости разработки в разах (значение меньше единицы, но больше нуля).

Так как разработка имеет одно исполнение, то

$$I_{финр}^{p} = \frac{Ф_{p}}{Ф_{\max}} = \frac{110843,85}{110843,85} = 1;$$

Для аналогов соответственно:

$$I_{финa1}^{a1} = \frac{Ф_{a1}}{Ф_{\max}} = \frac{161260,30}{110843,85} = 1,45;\ I_{финa1}^{a2} = \frac{Ф_{a1}}{Ф_{\max}} = \frac{145500,20}{110843,85} = 1,31;$$

Интегральный показатель ресурсоэффективности вариантов исполнения объекта исследования можно определить следующим образом:

$$I_{pi} = \sum a_i \cdot b_i \,,$$

где I_{pi}–интегральный показатель ресурсоэффективности для i-го варианта исполнения разработки;

a_i – весовой коэффициент *i*-го варианта исполнения разработки;

b_i^a, b_i^p – бальная оценка *i*-го варианта исполнения разработки, устанавливается экспертным путем по выбранной шкале оценивания;

n – число параметров сравнения.

Расчёт интегрального показателя ресурсоэффективности представлен ниже.

Таблица 3.6 –Сравнительная оценка характеристик вариантов исполнения проекта

ПО / Критерии	Весовой коэффициент параметра	Текущий проект	Аналог 1	Аналог 2
1.Соответствие нормативным документам	0,25	5	4	3
2.Удобство эксплуатации	0,2	5	4	3
3. Автономность	0,05	5	2	3
4. Надежность	0,2	5	4	3
5.Возможность модернизации	0,15	5	5	5
6. Конкурентоспособность разрабатываемой системы	0,15	5	1	4
ИТОГО	1	5	3,6	3,45

$I_{тп} = 5 \cdot 0,25 + 5 \cdot 0,2 + 5 \cdot 0,05 + 5 \cdot 0,2 + 5 \cdot 0,15 + 5 \cdot 0,15 = 5;$

Аналог 1 = $4 \cdot 0,25 + 4 \cdot 0,2 + 2 \cdot 0,05 + 4 \cdot 0,2 + 5 \cdot 0,15 + 1 \cdot 0,15 = 3,6;$

Аналог 2 = $3 \cdot 0,25 + 3 \cdot 0,2 + 3 \cdot 0,05 + 3 \cdot 0,2 + 5 \cdot 0,15 + 4 \cdot 0,15 = 3,45.$

Интегральный показатель эффективности вариантов исполнения разработки ($I^{p}_{финр}$) и аналога ($I^{ai}_{финаi}$) определяется на основании интегрального показателя ресурсоэффективности и интегрального финансового показателя по формуле:

$$I^{p}_{финр} = \frac{I^{p}_{m}}{I^{p}_{финр}};\ I^{ai}_{финаi} = \frac{I^{ai}_{m}}{I^{ai}_{финаi}};$$

В результате:

$$I^{p}_{финр} = \frac{I^{p}_{m}}{I^{p}_{финр}} = \frac{5}{1} = 5;\ I^{a1}_{фина1} = \frac{I^{a1}_{m}}{I^{a1}_{фина1}} = \frac{3,6}{1,45} = 2,48;\ I^{a2}_{фина2} = \frac{I^{a2}_{m}}{I^{a2}_{фина2}} = \frac{3,45}{1,31} = 2,63.$$

Сравнение интегрального показателя эффективности текущего проекта и аналогов позволит определить сравнительную эффективность проекта.

Сравнительная эффективность проекта:

$$Э_{ср} = \frac{I^{p}_{финр}}{I^{ai}_{финаi}}$$

Результат вычисления сравнительной эффективности проекта и сравнительная эффективность анализа представлены в таблице 3.6.1.

Таблица 3.6.1 – Сравнительная эффективность разработки

№	Показатели	Аналог 1	Аналог 2	Разработка
1	Интегральный финансовый показатель разработки	1,45	1,31	1
2	Интегральный показатель ресурсоэффективностиразработки	3,6	3,45	5
3	Интегральный показатель эффективности	2,48	2,63	5
4	Сравнительная эффективность вариантов исполнения	2,11	2	1

Таким образом, основываясь на определении ресурсосберегающей, финансовой, бюджетной, социальной и экономической эффективности исследования, проведя необходимый сравнительный анализ, можно сделать вывод о превосходстве выполненной разработки над аналогами.