Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Е.В. Бурькова

ПРЕДДИПЛОМНАЯ ПРАКТИКА

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2019

УДК 342.7
ББК 67.401 я7
Б 91

Рецензент – кандидат технических наук Р.Р. Галимов

Бурькова Е.В.
Б 91 Преддипломная практика: методические указания / Е.В. Бурькова; – Оренбургский гос. ун-т. Оренбург: ОГУ, 2019. – 47 с.

Методические указания содержат рекомендации по подготовке и проведению преддипломной практики обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность. Предназначены для обучающихся и руководителей преддипломной практики.

УДК 342.7
ББК 67.401 я7

Содержание

Введение

Проблемы обеспечения информационной безопасности становятся все более сложными и значимыми, находятся в центре внимания государства. В условиях постоянно меняющейся ситуации информационных угроз, стали востребованы новые знания и умения в сфере информационной безопасности. Требования, предъявляемые работодателями к специалисту в области информационной безопасности, достаточно высокие сегодня востребованы кадры нового поколения, способные быстро адаптироваться к постоянно изменяющимся угрозам информационной безопасности, обладающие высоким уровнем профессиональной компетентности.

Для обеспечения высокого качества подготовки специалистов в области информационной безопасности в университете должны быть реализованы следующие основные принципы:

− активное взаимодействие с работодателями сферы информационной безопасности как при разработке содержательной части образовательных программ, так и выполнении совместных проектов, предоставлении своей производственной базы для реализации практических задач;

− ориентация образовательного процесса на динамичные изменения профессиональной среды, синхронизацию с потребностями региона;

− усиление внимания на изучении нормативно-законодательных документов, национальных и международных стандартов в сфере обеспечения информационной безопасности;

− приобретение практических навыков использования средств защиты информации в условиях современных угроз информационной безопасности;

− создание инновационной образовательной среды, способствующей формированию у студентов мотивирующей системы участия в инновационной деятельности;

− развитие сотрудничества с Российскими и международными научными центрами, привлечение специалистов из таких центров для проведения совместных исследований [4].

В качестве перспективных путей повышения эффективности образовательного процесса применяются различные подходы, наиболее прогрессивным сочетанием является комптентностный и инновационный подходы.

Преддипломная практика бакалавров по направлению подготовки Информационная безопасность является важным этапом выполнения выпускной квалификационной работы, так как предполагает решение таких важных задач, как сбор и анализ исходных данных о предприятии, построение модели угроз информационной безопасности, проведение экспериментов и обработку результатов, а также и других задач, поставленных руководителем ВКР.

Данные методические указания предназначены для помощи обучающимся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность при прохождении преддипломной практики. Методические указания содержат сведения об основных этапах преддипломной практики, рекомендации по проведению обследования предприятия, примеры оформления результатов выполнения задач практики и отчета. Список источников литературы содержит 24 наименования и может быть использован обучающимися для решения задач преддипломной практики и выпускной квалификационной работы.

1 Общие положения проведения преддипломной практики

Преддипломная практика относится к обязательным дисциплинам (модулям) вариативной части блока 2 «Практики» основной образовательной программы бакалавриата по направлению 10.03.01 «Информационная безопасность».

Преддипломная практика предназначена для сбора и анализа данных, необходимых для решения задач и апробации полученных результатов научно-исследовательской работы в ходе выполнения ВКР.

Для прохождения преддипломной практики необходимо оформить следующие документы:

− договор с организацией, предоставляющей обучающемуся место практики;

− приказ о проведении преддипломной практики с указанием названия организации, даты начала и окончания практики, фамилии, имени, отчества и должности руководителя практики от кафедры.

В Федеральном государственном образовательном стандарте высшего образования по направлению подготовки 10.03.01 Информационная безопасность приводится список объектов профессиональной деятельности выпускников, освоивших программу бакалавриата:

− объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях угроз в информационной сфере;

− технологии обеспечения информационной безопасности объектов различного уровня, которые связаны с информационными технологиями, используемыми на этих объектах;

− процессы управления информационной безопасностью защищаемых объектов.

Организации, в которых проводится преддипломная практика, должны представлять собой объекты информатизации. В соответствии с документом ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», объект информатизации - это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Объектами проведения преддипломной практики могут быть:

- государственные и муниципальные предприятия и учреждения;
- некоммерческие и коммерческие организации;
- иные организации, подразделения.

Содержание преддипломной практики определяется требованиями к результатам обучения по практике, которые заложены в рабочей программе, и соответствуют компетенциям, указанным в учебном плане для данной дисциплины по направлению подготовки 10.03.01 Информационная безопасность.

В результате прохождения преддипломной практики обучающийся должен сформировать и закрепить знания:

- о социальной значимости своей будущей профессии при выполнении профессиональной деятельности в области обеспечения информационной безопасности;
- нормативно-правовых основ законодательства в области информационной безопасности ФСБ, ФСТЭК;
- основных источников и носителей информации;
- характеристик защищаемой информации;
- основных угроз безопасности для информации;
- основных этапов анализа исходных данных объекта защиты;

− категорий защищаемой информации, категорий объектов по уровню важности;

− источников угроз информационной безопасности,

− методов и средств обеспечения информационной безопасности, их классификацию, назначение, принципы работы, технико-экономические характеристики и особенности применения.

− нормативных правовых актов, методических документов, национальных стандартов в области защиты информации ограниченного доступа и аттестации выделенных помещений на соответствие требованиям по защите информации;

− технических описаний и инструкций по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам;

− требований к содержанию организационно-распорядительных документов организации.

− административного уровня комплексной защиты;

− политику информационной безопасности;

− основных программно-технических мер;

− принципов организации и управления мероприятиями комплексной защиты информации информационно-вычислительных систем и телекоммуникаций.

Постановка задач по преддипломной практике разрабатывается руководителем практики от кафедры вычислительной техники и защиты информации и включает ряд задач выпускной квалификационной работы индивидуально для каждого обучающегося.

Результаты практики оформляются в виде отчета. Отчет должен быть сдан руководителю от предприятия и руководителю от кафедры в установленные графиком сроки. Руководитель практики от предприятия предоставляет отзыв о работе обучающегося, заверенный подписью и печатью. Руководитель практики от кафедры оценивает выполнение поставленных задач в соответствии с установленным в фонде оценочных средств порядком оценивания.

2 Цели и задачи преддипломной практики

2.1 Цель практики

Целью преддипломной практики является ознакомление со структурой и деятельностью предприятия, сбор и анализ исходных данных для выполнения задач ВКР, подготовка теоретического и практического материала, апробация результатов исследований, статистическая обработка данных, подготовка отчета.

Виды профессиональной деятельности, к которым ведется подготовка бакалавров по направлению 10.03.01 Информационная безопасность:

- эксплуатационная,
- проектно-технологическая,
- экспериментально-исследовательская,
- организационно-управленческая.

2.2 Задачи практики

В соответствии с перечисленными видами профессиональной деятельности определяются задачи преддипломной практики.

В рамках эксплуатационной деятельности реализуются следующие задачи:

- установка, настройка, эксплуатация компонентов системы информационной безопасности;
- изучение технических описаний и инструкций (руководства) по эксплуатации технических средств защиты информации от утечки по техническим каналам и программно-математических воздействий;
- участие в проведении аттестации объектов информатизации и аудите информационной безопасности.

В рамках проектно-технологической деятельности реализуются следующие задачи:

- сбор и анализ сведений о структуре и деятельности предприятия;
- составление перечня защищаемых ресурсов;

− сбор и анализ исходных данных о средствах защиты информации на предприятии;

− анализ уязвимостей, разработка модели угроз и модели нарушителя безопасности информации;

− проведение проектных расчетов элементов систем обеспечения информационной безопасности;

− анализ нормативно-правовой документации по защите информации для данного объекта;

− участие в разработке технологической и эксплуатационной документации;

− проведение технико-экономического обоснования проекта.

В рамках экспериментально-исследовательской деятельности реализуются следующие задачи:

− поиск и анализ научно-технической информации по тематике ВКР, включая статьи, патенты, монографии, авторефераты диссертаций отечественных и зарубежных ученых;

− проведение экспериментов по заданной методике;

− обработка и анализ результатов экспериментов.

В рамках организационно-управленческой деятельности реализуются следующие задачи:

− изучение организационно-распорядительной документации по информационной безопасности;

− участие в модернизации системы управления информационной безопасностью;

− изучение и обобщение опыта работы других учреждений, организаций, предприятий в области защиты информации;

− участие в работах по контролю эффективности реализации политики информационной безопасности объекта защиты.

2.3 Контрольные вопросы

1 Дать определение понятия «объект информатизации». Привести примеры объектов информатизации.

2 Назвать объекты профессиональной деятельности бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

3 Что входит в состав эксплуатационной деятельности бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

4 Перечислить виды работ, входящие в проектно-технологическую деятельность бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

5 Охарактеризовать виды работ, входящие в экспериментально-исследовательскую деятельность бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

6 Что входит в состав организационно-управленческой деятельность бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

7 Назвать и пояснить категории объектов информатизации по уровню важности.

8 Назвать и охарактеризовать основные виды защищаемых ресурсов объекта информатизации.

9 В соответствии с каким нормативным документом необходимо определять перечень сведений конфиденциального характера? Дать характеристику документа.

10 Привести определение основных и дополнительных характеристик безопасности информации.

3 Порядок прохождения преддипломной практики

Преддипломная практика проводится в соответствии с утвержденным учебным планом и рабочей программой практики для обучающихся по направлению подготовки 10.03.01 Информационная безопасность.

На предприятии (организации) прохождения практики необходимо:

− оформление приказа по организации о приеме обучающегося на определенную должность, допуске его к сведениям, необходимым для выполнения задач ВКР;

− приказ о назначении руководителя практики от соответствующего подразделения организации;

− оформление пропуска в организацию, предусмотренного внутренним распорядком;

− изучение правил внутреннего трудового распорядка;

− изучение правил пожарной безопасности, охраны труда и техники безопасности на рабочем месте;

− правил действий в экстремальных условиях и при признаках террористических действий и подаваемых в этих случаях сигналах тревоги;

− ознакомление обучающегося с его должностной инструкцией.

Руководитель практики от кафедры обязан:

− разработать индивидуальное задание;

− взаимодействовать с обучающимися по вопросам прохождения практики и подготовки отчета;

− проверить и принять отчет обучающихся по практике.

Руководитель практики от организации обязан предоставить допуск к материалам, необходимым для решения поставленных задач практики, проводить контроль за всеми действиями обучающегося, консультировать его по возникающим вопросам, допускать к участию в работе по организации и проведению мероприятий по обеспечению информационной безопасности в

организации, оказывать содействие в проведении экспериментов по заданным методикам.

Обучающийся, проходящий практику, обязан:

- своевременно выполнять поставленные задачи практики;
- регулярно посещать организацию практики в соответствии с приказом;
- подчиняться правилам внутреннего распорядка организации;
- своевременно предоставлять руководителю от кафедры результаты выполнения задач практики;
- вести дневник и записывать в нем состав выполняемых задач за каждый день;
- самостоятельно разработать отчет по практике, содержащий развернутое описание выполненных задач индивидуального задания.

3.2 Контрольные вопросы

1 Какие обязательные документы для прохождения преддипломной практики должны быть оформлены в университете?

2 Какие обязательные документы для прохождения преддипломной практики должны быть оформлены в организации прохождения практики?

3 Каковы обязанности руководителя практики от кафедры?

4 Каковы обязанности руководителя практики от организации?

5 Что входит в обязательный перечень задач обучающегося при поступлении в организацию для прохождения практики?

6 Какие документы должен оформить обучающийся по окончании прохождения практики?

4 Содержание практики

4.1 Изучение структуры и деятельности предприятия

Цель:

− построение структурной схемы предприятия или отдельного подразделения, подлежащего защите в рамках задач ВКР;

− детализация конкретного объекта защиты информации в общей структуре предприятия;

− составление перечня решаемых задач на объекте защиты;

− разработка перечня защищаемых ресурсов в соответствии с деятельностью предприятия с указанием категории защищаемой информации;

− определение категории защищаемого объекта по уровню важности.

Для выполнения задач практики, поставленных руководителем, необходимо провести изучение организационной структуры предприятия, построение иерархической структурной схемы всех подразделений; изучение деятельности, осуществляемой на предприятии, построение перечня основных задач, проведение анализа информационных процессов на предприятии. Изучение характеристик защищаемой информации предприятия. Изучение правил разграничения доступа к защищаемой информации на предприятии.

Изучение организационной структуры предприятия необходимо для определения места заданного защищаемого объекта (подразделения) в общей структуре. Пример схемы организационной структуры приведен на рисунке 4.1.

Для характеристики деятельности предприятия необходимо провести анализ решаемых задач и результаты оформить в виде таблицы по примеру таблицы 4.1.

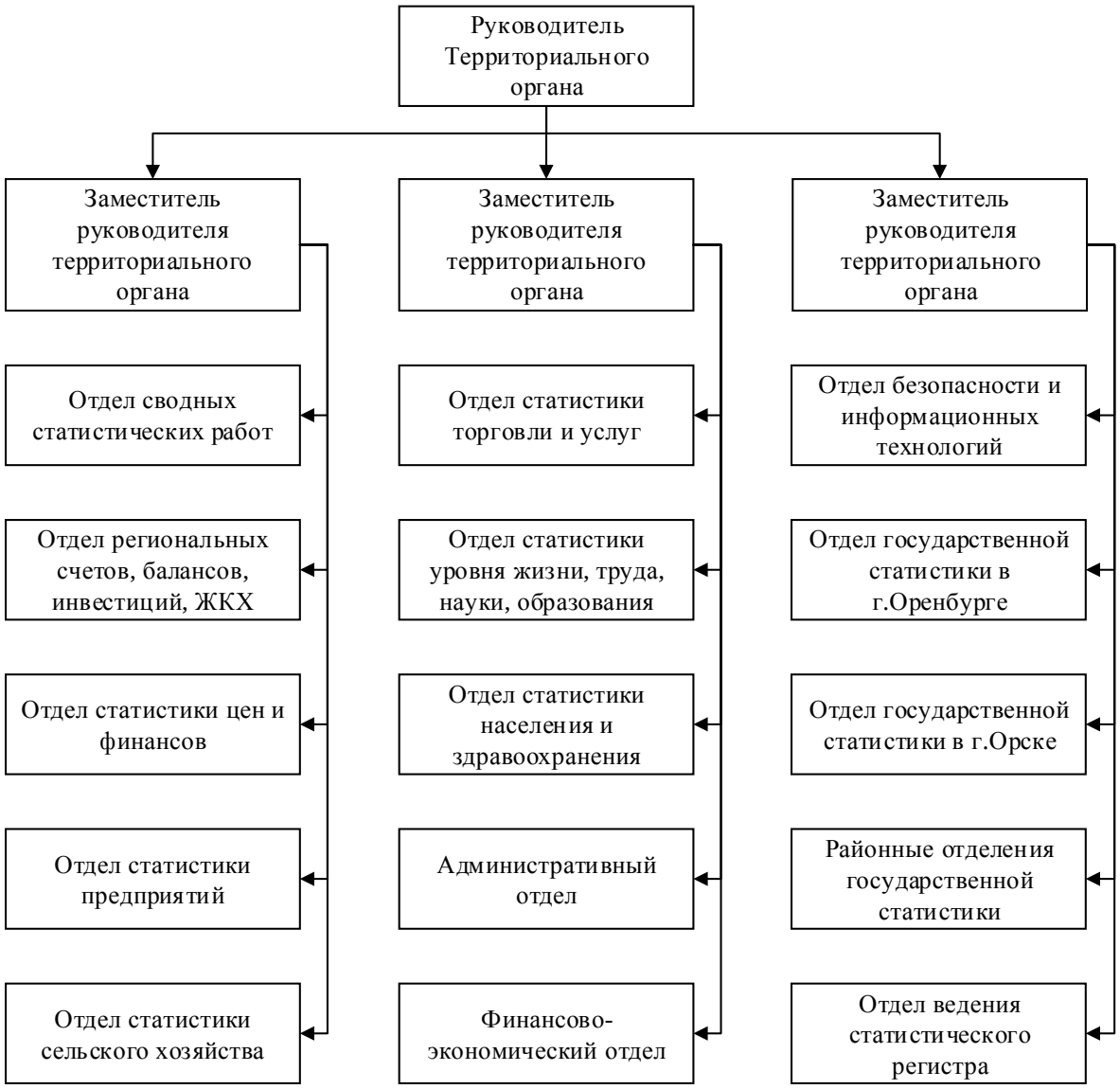


Рисунок 4.1 - Схема организационной структуры организации

Таблица 4.1 – Описание деятельности подразделений объекта защиты

Наименование отдела	Решаемые задачи	Вид защищаемой информации
Отдел статистики торговли и услуг	Формирует статистическую информацию об экономических процессах в Оренбургской области по торговле и услугам для последующего представления в установленном порядке в Росстат	Для служебного пользования

Продолжение таблицы 4.1

Отдел безопасности и информационных технологий	Внедряет информационные технологии в работу организации, с целью создания интегрированных информационных ресурсов государственной статистики и организации доступа к ним на основе использования технологий хранилищ данных, а также обеспечение информационной безопасности информационных технологий	Для служебного пользования
Отдел статистики предприятий	Формирует официальные статистические показатели производственной деятельности предприятий, их структуре, демографии, потреблению топливно-энергетических ресурсов.	Для служебного пользования

Необходимо провести анализ технической, экономической и социальной значимости решаемых задач для последующего определения категории объекта защиты по уровню важности.

Характеристика деятельности защищаемого объекта включает в себя определение его функционально-отраслевой принадлежности. Категорирование объекта информатизации может быть осуществлено: по назначению, по степени пожаро- и взрывоопасности, по виду потерь, по масштабу потенциальных потерь, по объему производства, по количеству персонала и т.д. [5].

По функционально-отраслевой принадлежности все объекты делятся на:

- производственные;
- строительные;
- транспортные;
- топливно-энергетического комплекса;
- оборонно-промышленного комплекса;
- социального назначения;
- культурного назначения.

По виду потерь:

− политические (определяются возможным подрывом авторитета власти, возникновением политической нестабильности);

− людские (выражаются в нанесении вреда жизни и здоровью людей);

− финансовые (определяются материальными потерями);

− экологические (нанесение вреда природным ресурсам);

− культурные (потери, свзанные с утратой художественных ценностей, памятников архитектуры и т.д.);

По масштабу потенциальных потерь:

− локальный (в пределах одного объекта);

− местный (в пределах населенного пункта);

− территориальный (в пределах территории субъекта России);

− региональный (затрагивающий масштабы региона);

− государственный (затрагивает более двух субъектов РФ);

− межгосударственный (выходит за пределы страны).

При анализе деятельности защищаемого объекта необходимо определить состав, содержание и местонахождение защищаемых ресурсов: информации, материальных ценностей, так как в зависимости от ценности этих ресурсов формируется вывод о видах и масштабах потенциального ущерба при реализации возможных угроз безопасности [3, 5].

К защищаемым ресурсам относятся:

− персонал компании (руководящие работники, производственный персонал, имеющий непосредственный доступ к финансам, валюте, ценностям, хранилищам, осведомленные в сведениях, составляющих коммерческую тайну, работники внешнеэкономических служб и другие);

− финансовые средства;

− информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы

данных, программное обеспечение, информативные физические поля различного характера;

− средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

− материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

− технические средства и системы охраны и защиты материальных и информационных ресурсов.

Цель категорирования на современном этапе была сформулирована как «создание системы категорирования, предполагающей дифференциацию требований к системе антитеррористической и противокриминальной защиты объектов, обеспечивающей минимально необходимые и достаточные уровни безопасности объектов в соответствии с их категориями потенциальной опасности, с учетом критериев оценки возможного ущерба интересам личности, общества и государства, который может быть нанесен преступными действиями в случае невыполнения требований, предъявляемых к системе защиты объекта» [3].

Категории объектов по уровню важности определяют в соответствии с РД 78.36.003-2002:

− **объекты группы А:** особо важные, повышенной опасности и жизнеобеспечения, противоправные действия на которых могут привести к крупному ущербу государству, экологии или владельцу имущества;

− **объекты группы Б:** важные объекты, хищения на которых могут привести к ущербу в размере свыше 500 МРОТ.

Пример категорирования объекта приведен в таблице 4.2.

Таблица 4.2 – Категорирование защищаемого объекта

Информационный признак	Категория исследуемого объекта
По функционально-отраслевой принадлежности	Производственный объект
По виду возможного ущерба	Финансовые
По масштабу возможного ущерба	Локальный
По важности объекта	Особо важный объект А1
По категории информации	Персональные данные, служебная и коммерческая тайна
По пожаро- и взрывоопасности	Д - пониженной пожароопасности
По численности персонала свыше 500 человек	Менее 500 человек
По материальным активам свыше 500 МРОТ	Свыше 500 МРОТ

4.2 Сбор и анализ исходных данных о защищаемом объекте

Цель:

- построение плана объекта защиты;
- построение схемы информационной сети;
- формирование перечня программных и технических средств обработки информации;
- разработка структурной модели защищаемой информации;
- разработка перечня защищаемых ресурсов;
- разработка схемы информационных потоков и описание;
- анализ средств защиты информации на данном объекте.

4.2.1 Построение плана объекта защиты

Для решения задач ВКР требуется построение плана объекта защиты с указанием места расположения защищаемых ресурсов.

Пример плана защищаемого объекта приведен на рисунке 4.2.

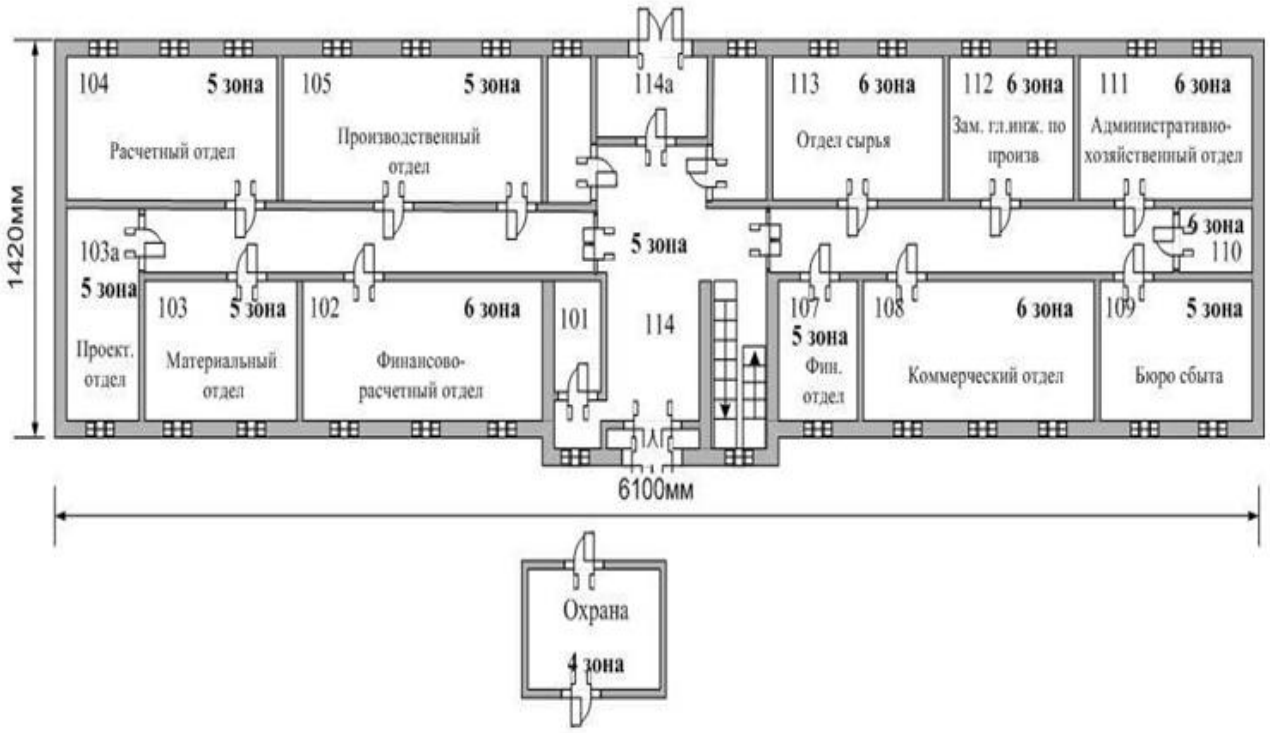


Рисунок 4.2 - Пример плана защищаемого объекта

На данном плане показаны кабинеты, относящиеся к отделам организации и указаны зоны по уровню доступа. В примере присутствуют только зоны 5 и 6.

По уровню доступа различают шесть видов зон:

- свободная (1);
- наблюдаемая (2);
- регистрационная (3);
- режимная (4);
- усиленной защиты (5);
- наивысшей защиты (6).

Каждая зона характеризуется требованиями к уровню безопасности находящейся в ней информации, или других защищаемых ресурсов. Безопасность информации в зоне зависит от количества и качества рубежей защиты, эффективности применяемых средств и мероприятий защиты [22].

Пример характеристики защищаемых информационных ресурсов приведен в таблице 4.3.

Таблица 4.3 –Характеристика защищаемых информационных ресурсов

Наименование информационного ресурса	Категория информации	Месторасположение	Значимость	№ зоны по уровню доступа
Документация технологическая и конструкторская	Коммерческая тайна	Производственно-технический отдел (кабинет начальника производственно-технического отдела)	Высокая	6
Конструкторская документация	Коммерческая тайна	Кабинет главного инженера	Высокая	6
Финансовая документация	Коммерческая тайна	Финансово-расчетный отдел (кабинет заместителя главного бухгалтера)	Высокая	5
Персональные данные сотрудников	Персональные данные	Кабинет заместителя генерального директора по персоналу	Высокая	6
Сведения о системе защиты	Коммерческая тайна	Кабинет заместителя генерального директора по безопасности	Высокая	6
Финансовая, конструкторская документация, приказы по предприятию	Служебная тайна	Кабинет генерального директора	Высокая	6

Защищаемая информация может быть расположена на разнообразных носителях подвергаться как автоматизированной, так и неавтоматизированной

обработке. Обработка информации - действия (операции) с данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение [16].

4.2.2 Построение схемы информационной сети

Все информационные ресурсы сосредоточены в информационных системах. Информационная система представляет собой совокупность данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких данных с использованием средств автоматизации или без использования таких средств.

В соответствии с выше сказанным, важным защищаемым объектом на предприятии является информационная вычислительная сеть, так как вся информация хранится и обрабатывается в ней. На рисунке 4.3 приведена схема информационной сети организации.

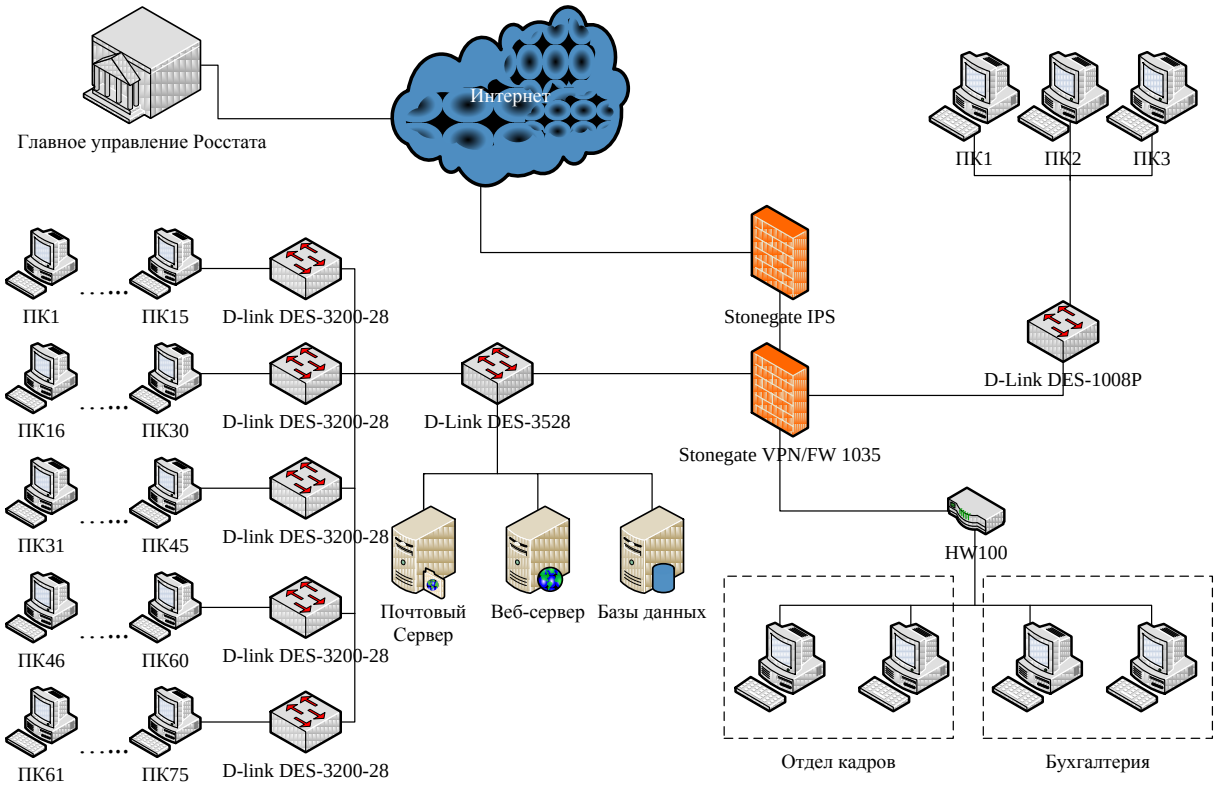


Рисунок 4.3 - Схема информационной сети организации

На каждом предприятии построена и функционирует своя информационная вычислительная сеть, которая может иметь или не иметь выход в глобальную сеть Интернет. Для проектирования системы защиты информации важно построить схему вычислительной сети и изучить ее состав и информационные потоки.

Схема сети должна быть снабжена описанием ее состава. Пример перечня технических средств информационной сети приведен в таблице 4.4.

Таблица 4.4 – Перечень технических средств информационной сети

Наименование	Функция	Фирма - изготовитель	Количество
Acer V223	Монитор	Acer V223	85
Intel Core 2 Duo	Рабочая станция	E-Machines	85
Cisco SPA512G	IP-телефон	Cisco	75
D-link DES-3200-28	Коммутатор	D-Link	5
D-Link DES-3528	Коммутатор	D-Link	1
D-Link DES-1008P	Коммутатор	D-Link	1
HP Laser Jet P1005	Принтер	HP	35
SYS-6027B-URF	Сервер	SuperMicroRackmount	3
ViPNet Coordinator HW100	Средство шифрования	ViPNet	1
Stonegate VPN 1035	VPN	Stonegate	1
Stonegate FW 1035	Firewall	Stonegate	1
Stonegate IPS	Система защиты от вторжений	Stonegate	1

Программное обеспечение информационной сети должно быть проанализировано на предмет осуществления защиты основных свойств информации: конфиденциальности, целостности и доступности.

Пример анализа программного обеспечения информационной сети организации приведен в таблице 4.5.

Таблица 4.5 – Анализ программного обеспечения организации

Наименование	Характеристики Безопасности		
	Конфиденциальность	Целостность	Доступность
Microsoft Windows Server 2008	+	+	+
Microsoft SQL Server	+	+	+
Microsoft Windows 7	+	+	+
Microsoft Office 2010	-	+	-
Dallas Lock 7.5	+	+	+
ViPNet Coordinator	+	+	+
ViPNet Client	-	+	+
ViPNet CUSTOM 2.8	+	+	+
Kaspersky Endpoint Security 10	+	+	+
VMware vSphere	+	+	-
Microsoft Baseline Security Analyzer	-	+	+
ФИКС-Unix 1.0	-	+	+

Анализ программного обеспечения необходим для проведения аудита безопасности информационных ресурсов в организации и выработки рекомендации по совершенствованию системы защиты информации, либо разработки концептуальных решений по проведению каких-либо мероприятий защиты.

4.2.3 Разработка схемы информационных потоков

Для проектирования системы и реализации мероприятий по защите информации необходимо проанализировать информационные процессы в данной организации и построить схему информационных потоков между подразделениями.

Пример схемы информационных потоков приведен на рисунке 4.4.

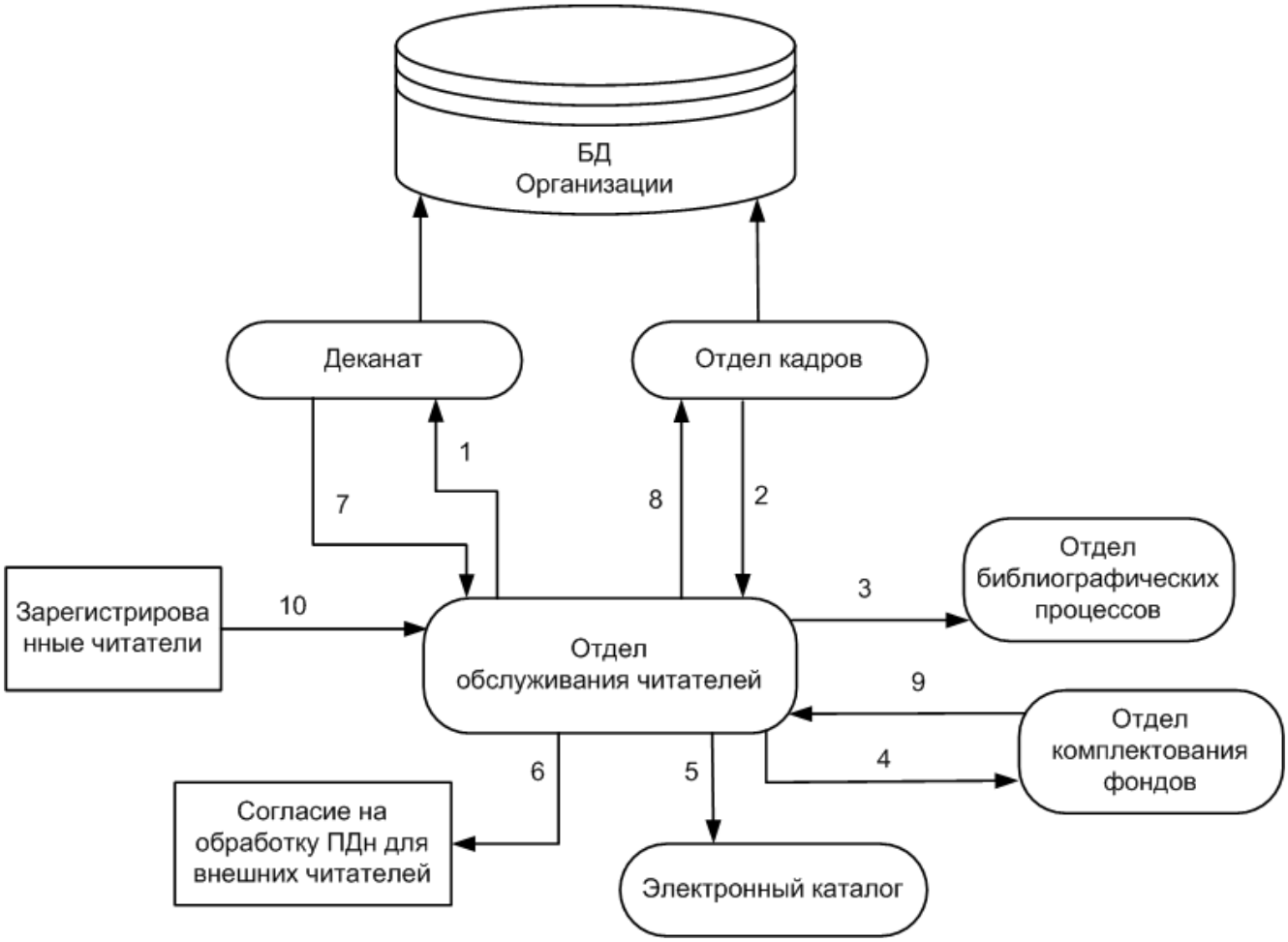


Рисунок 4.4 - Схема информационных потоков организации

В таблице 4.6 приведено описание информационных потоков организации.

Таблица 4.6 – Описание информационных потоков организации

№ потока	Исходящие	Входящие	Содержание потока	Категория
1	2	3	4	5
1	Отдел обслуживания читателей	Деканат	Данные о контингенте студентов	ПДн

Продолжение таблицы 4.6

1	2	3	4	5
2	Отдел кадров	Отдел обслуживания читателей	Данные о контингенте сотрудников, аспирантов	ПДн
3	Отдел обслуживания читателей	Отдел библиографических процессов	Статистика посещаемости, качественном составе	Служебная информация
4	Отдел обслуживания читателей	Отдел комплектования фондов	Статистика о востребованности литературы	Служебная информация
5	Отдел обслуживания читателей	Электронный каталог	Данные о наличии литературы	Служебная информация
6	Отдел обслуживания читателей	Внешние читатели	Согласие на обработку ПДн	ПДн
7	Деканат	БД организации	Данные о контингенте	ПДн
8	Отдел обслуживания читателей	Отдел кадров	Данные о должниках литературы	ПДн
9	Отдел комплектования фондов	Отдел обслуживания читателей	Учет экземпляров литературы	Служебная информация
10	Зарегистрированные читатели	Отдел обслуживания читателей	Электронный пропуск	Служебная информация

Схема информационной сети определяется требованиями управленческого аппарата к оперативности информационного обмена между структурными подразделениями организации. Высокие требования к оперативности информации в управлении объектом привело к созданию сетевых технологий, которые развиваются в соответствии с требованиями современных условий функционирования организации [1].

Определение автоматизированной информационной технологии определяется следующими факторами:

- отраслевой принадлежностью предприятия или организации;
- типом предприятия или организации;
- производственно-хозяйственной или иной деятельностью;
- принятой моделью управления организацией или предприятием;
- решаемыми задачами в управлении;
- существующей информационной инфраструктурой.

На малых предприятиях различных сфер деятельности информационные технологии, как правило, связаны с решением задач бухгалтерского учета, накоплением информации по отдельным видам бизнес-процессов, созданием информационных баз данных по направленности деятельности фирмы и организации телекоммуникационной среды для связи пользователей между собой и с другими предприятиями и организациями.

В средних организациях (предприятиях) важное значение для управленческого звена имеет электронный документооборот и отношение его к определенным бизнес-процессам. Характерной чертой таких организаций (предприятий, фирм) является расширение круга функциональных задач, связанных с деятельностью фирмы, организация автоматизированных хранилищ и архивов информации, которые позволяют накапливать документы в различных форматах, предполагают наличие их структуризации, возможностей поиска, защиты информации от несанкционированного доступа и т.д.

В крупных организациях (предприятиях) информационная технология строится на базе современного программно-аппаратного комплекса, включающего телекоммуникационные средства связи, многомашинные комплексы, развитую архитектуру «клиент-сервер», применение высокоскоростных корпоративных вычислительных сетей. Для крупных организаций характерны две формы управления – централизованная и децентрализованная [23].

Централизованное управлением характеризуются распределением функций среди структурных подразделений с жесткой координацией производственно-хозяйственной деятельности. Децентрализованная форма характеризуется выделением внутри организации стратегических единиц, деятельность которых поддается самостоятельному планированию.

4.2.4 Анализ средств защиты информации в организации

В рамках сбора исходных данных для выполнения ВКР необходимо провести анализ имеющихся в организации средств защиты. Причем все средства защиты могут быть сгруппированы в следующие подсистемы:

- подсистема физической защиты;
- подсистема программно-аппаратной защиты;
- организационные мероприятия.

Если требуется проводить анализ защиты информационной вычислительной сети, то рассматривают схему сети с указанием имеющихся средств защиты. Для анализа средств физической защиты необходимо рассмотреть все рубежи защиты. Схема анализа средств защиты сети организации приведена на рисунке 4.5.

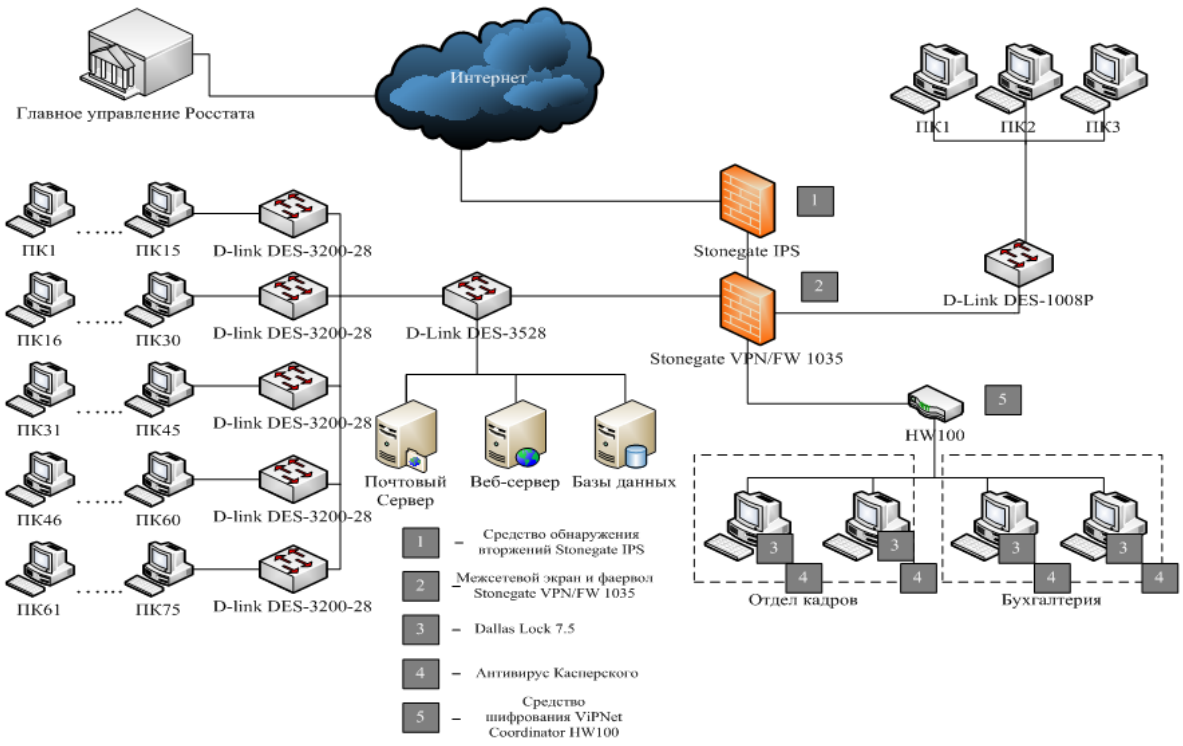


Рисунок 4.5 – Схема анализа средств защиты сети организации

На данной схеме показаны программно-аппаратные средства защиты, функционирующие в организации.

Далее в таблице 4.7 приведен анализ подсистем защиты информации в приведенной сети [6].

Таблица 4.7 – Анализ подсистем существующих средств защиты информации

Наименование подсистемы	Наименование средства ЗИ	Реализованные функции	Уровень защиты	Недостатки
1	2	3	4	5
Подсистема идентификации и аутентификации субъектов доступа и объектов доступа	Встроенные средства Microsoft Windows Server	Идентификация и аутентификация пользователей, являющихся работниками оператора	Средний	Нет
Подсистема управления доступом субъектов доступа к объектам доступа	Dallas Lock 7.5	Разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Средний	Нет
Подсистема защиты среды виртуализации	VMware vSphere	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Средний	Нет
Подсистема защиты машинных носителей персональных данных	Организационные меры: инструкция по защите информационных ресурсов	Уничтожение или обезличивание персональных данных на машинных носителях при их передаче между пользователями или в сторонние организации, а также контроль уничтожения или обезличивания	Средний	Нет
Подсистема обнаружения вторжений	Stonegate IPS	Обнаружение вторжений	Низкий	Отсутствует обновление базы решающих правил

Продолжение таблицы 4.7

1	2	3	4	5
Подсистема регистрации событий безопасности	Встроенные средства Microsoft Windows Server	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Средний	Нет
Подсистема антивирусной защиты	Антивирус Касперского	Реализация антивирусной защиты, обновление баз данных признаков вредоносных программ	Низкий	Нет
Подсистема анализа защищенности персональных данных	Microsoft Baseline Security Analyzer	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Низкий	Отсутствует контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей
Подсистема обеспечения целостности персональных данных	ФИКС-Unix 1.0	Контроль целостности персональных данных, содержащихся в базах данных информационной системы	Средний	Нет
Подсистема обеспечения доступности персональных данных	ФИКС-Unix 1.0	Резервирование технических средств, программного обеспечения, каналов передачи информации,	Средний	Нет
Подсистема защиты информационной системы, ее средств, систем связи и передачи данных	ViPNet Coordinator, Stonegate VPN/FW 1035	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю	Низкий	Отсутствует обеспечение подлинности сетевых соединений, в том числе для защиты от подмены сетевых устройств и сервисов

В результате анализа существующих в организации средств защиты необходимо сделать вывод о достаточности уровня защищенности информации на данном объекте и сформулировать направления совершенствования системы информационной безопасности организации.

4.3 Построение модели угроз и модели нарушителя

Процесс формирования модели угроз начинается с этапа анализа источников угроз безопасности для защищаемых ресурсов исследуемой организации. Все источники угроз можно разделить на группы: антропогенные, техногенные, стихийные. В соответствии с этим делением проводится анализ уязвимостей и угроз безопасности. Классификация источников угроз физической безопасности приведена на рисунке 4.6.

Рисунок 4.6 – Классификация источников угроз физической безопасности

В качестве антропогенных источников угроз выступает нарушитель: внешний и внутренний. Составление модели нарушителя информационной безопасности является частью процесса формирования модели угроз для заданного предприятия. Модель нарушителя разрабатывается с учетом таких характеристик:

- цели и задачи вероятного нарушителя;
- степень принадлежности вероятного нарушителя к объекту;
- степень осведомленности вероятного нарушителя об объекте;
- степень осведомленности нарушителя о системе защиты объекта;
- степень профессиональной подготовленности вероятного нарушителя;
- степень технической оснащенности вероятного нарушителя;
- владение вероятным нарушителем различными способами маскировки;
- способ проникновения вероятного нарушителя на объект.

Пример неформализованной модели нарушителя приведен в таблице 4.8.

Таблица 4.8 - Типовая модель нарушителя

Тип нарушителя	Категория	Подготовленность нарушителя								
		Психофизическая			Техническая			Осведомленность		
		В	С	Н	В	С	Н	В	С	Н
1	2	3	4	5	6	7	8	9	10	11
Внутренние	Сотрудники, имеющие санкционированный доступ к материальным ценностям		+			+		+		
	Сотрудники, имеющие доступ к финансовым ценностям		+			+		+		
	Сотрудники, имеющие доступ к служебной информации	+			+			+		

Продолжение таблицы 4.8

1	2	3	4	5	6	7	8	9	10	11
	Сотрудники, имеющие доступ к элементам системы защиты		+			+			+	
	Обслуживающий персонал (охрана, инженерно-технические службы)			+		+			+	
Внешние	Уполномоченный персонал разработчиков, который имеет право на техническое обслуживание	+			+			+		
	Уволенный сотрудник		+			+			+	
	Недобросовестные партнеры		+			+			+	
	Конкуренты		+				+		+	
	Посетители			+			+			+

Модель угроз безопасности - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Для построения модели угроз безопасности необходимо применить руководящие документы ФСТЭК [2, 14, 17, 18, 19].

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Пример модели угроз безопасности ПДн приведен в таблице 4.9.

Таблица 4.9 – Пример модели угроз безопасности ПДн

Угроза	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
Угрозы от утечки по техническим каналам				
Угрозы утечки акустической информации	Маловероятно (0)	Низкая	Низкая	Неактуальная
Угрозы утечки видовой информации	Маловероятно (0)	Низкая	Низкая	Неактуальная
Угрозы утечки информации по каналам ПЭМИН	Маловероятно (0)	Низкая	Низкая	Неактуальная
Угрозы несанкционированного доступа к информации				
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
Кража ПЭВМ	Маловероятно (0)	Низкая	Низкая	Неактуальная
Кража носителей информации	Низкая (2)	Средняя	Средняя	Актуальная
Кража ключей доступа	Низкая (2)	Средняя	Средняя	Актуальная
Кража, модификация, уничтожение информации	Средняя (5)	Средняя	Средняя	Актуальная
Несанкционированное отключение средств защиты	Маловероятно (0)	Низкая	Средняя	Неактуальная
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением аппаратно-технических и программных средств				
Действия вредоносных программ	Средняя (5)	Средняя	Средняя	Актуальная
Недекларированные возможности прикладного ПО	Средняя (5)	Средняя	Средняя	Актуальная

По результатам построения модели угроз информационной безопасности необходимо проанализировать насколько существующие в организации средства защиты нейтрализуют угрозы [9]. Пример такого анализа представлен в таблице 4.10.

Таблица 4.10 – Пример анализа средств защиты от актуальных угроз

Угроза	Средства защиты				
	Межсетевое экранирование и система обнаружения вторжений (Cisco ASA5505-BUN-K9 + Cisco IPS 4510)	Обнаружение уязвимостей сети с помощью специализированных программ-сканеров (XSpider 7.8)	Разграничение доступа (механизмы управления доступом в ОС Windows) и организация контролируемой зоны с пропускным режимом	Использование виртуальных частных сетей (IPsec)	Антивирусные средства защиты (Kaspersky Endpoint Security)
Внедрение вредоносных программ	+	-	+	-	+
Анализ сетевого трафика	+	-	-	+	-
Осуществление НСД с применением штатных средств операционной системы и прикладных программ;	-	-	+	-	-
«Отказ в обслуживании»	+	-	+	-	-
Угроза выявления паролей	-	-	+	-	+
Внедрение вредоносных программ по сети	+	-	-	-	+

По результатам анализа можно сделать вывод о необходимости принятия дополнительных мер по защите информационных и других ресурсов организации, выработать направления защиты и разработать концептуальную модель системы защиты.

4.4 Сбор и анализ научно-технической информации

Цель:

- поиск публикаций по теме ВКР;
- анализ методов различных ученых, используемых для решения данной задачи;
- выбор одного или нескольких методов для решения задач ВКР;
- составление библиографического списка.

Научно-техническая информация — согласно ГОСТ 7.0–99 СИБИД «Информационно библиотечная деятельность, библиография. Термины и определения», – информация, получаемая и (или) используемая в области науки и (или) техники. Научно-техническая информация подразделяется на три потока:

1) патентную литературу, являющуюся основной формой обмена, т.к. все новое в области науки и техники официально оформляется в виде патента и его производных форм;

2) периодические издания, целью которых является опубликование наиболее актуальных научных разработок, имеющих теоретическую и практическую значимость, например: отраслевые бюллетени, содержащие рефераты, аннотации и названия; отраслевые научно-технические журналы, содержащие дискуссионные, проблематичные и отчетные статьи в рамках научных проектов и конкурсов; библиографические указатели с названием тем, изобретений и предметов промышленной продукции;

3) информационная база диссертаций;

4) российские и зарубежные базы научных публикаций.

Поиск публикаций по тематике выпускной квалификационной работы необходимо проводить, используя Российскую базу научных публикаций РИНЦ и портал электронной научной библиотеки elibrary.ru. Для этого надо пройти процедуру регистрации на сайте https://elibrary.ru [15] и воспользоваться возможность расширенного поиска по заданной тематике публикаций, размещенных на портале научной библиотеки. На этом портале предоставляется

возможность найти и скопировать научные статьи, которые имеют полнотекстовое размещение, а также найти научные журналы по интересующей тематике [7, 12]. Тексты авторефератов диссертаций по интересующей тематике и самих диссертаций можно найти на портале Высшей аттестационной комиссии [8].

Проанализировав найденные публикации, необходимо разработать классификацию применяемых методов и выявить их достоинства и недостатки.

Пример анализа методов приведен в таблице 4.11.

Таблица 4.11 – Анализ методов решения задачи

Метод оценки защищенности ИС	Достоинства	Недостатки
1	2	3
По классам защищённости	Простота применения. Универсальность (может быть использован для АС разного профиля). Высокая степень документированности. Повсеместно используемый как для государственных учреждений, так и для частных организаций.	При наличии большого числа стандартов отсутствует единая терминология, которая отслеживает изменения в области защиты информации. Отсутствие количественных показателей и единых требований к функционированию СЗИ.
На основе модели комплекса механизмов защиты	Количественные показатели. Получение двух оценок защищённости: 1) обеспечиваемой конкретным СЗИ. 2) всей системы в целом. Позволяет воздействовать на показатель защищённости, изменяя расположение механизмов защиты по уровням СЗИ.	Необходимость проведения сложных математических расчётов. Статичный характер оценки защищённости. Не учитываются такие показатели как ущерб от атак и частота осуществления атак. Предположение о снижении количества актуальных угроз по мере приближения к объекту защиты не всегда справедливо.
На основе семантических показателей защищённости	Отсутствие каких-либо математических расчётов. Воспроизводится при наличии необходимого количества статистических данных. Учитываются такие показатели как «ущерб от атаки» и «частота реализации».	Результат оценки только в качественной форме. Оценка базируется только на статистике и субъективном мнении эксперта. Не даёт рекомендаций на изменение состава механизмов защиты и структуры СЗИ.

Продолжение таблицы 4.11

1	2	3
На основе тестов на проникновение	Позволяет получить «реальную» оценку уровня защищённости за счёт имитации действий нарушителя. Помогает обнаружить погрешности в настройке и эксплуатации. установленных средств защиты. Даёт рекомендации по повышению уровня защищённости и модернизации СЗИ.	Необходимо участие квалифицированного специалиста. Высокие временные затраты по сравнению с другими методами. Стандарт проведения тестирования и сопутствующая техническая документация не переведены на русский язык.

В результате поиска и анализа публикаций по теме ВКР обучающийся составляет обзор существующих исследований и методов решения данной задачи. Этот этап является важным, так как для разработки своей концепции необходимо знать, какие методы применялись и какие результаты были получены различными учеными в этой области. Проведение такого анализа позволит добиться разработки решения, обладающего научной новизной, теоретической и практической значимостью.

Библиографический список составляется в соответствии с ГОСТ 7.1, ГОСТ 7.82. Пример списка:

1 Аверченков, В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – М.: Флинта, 2016. – 124 с.

2 Алексашина, М.Н. Защита персональных данных как условие обеспечения безопасности личности / М.Н.Алексашина // Право и безопасность. - 2014. - № 1. С. 68-73.

3 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : Руководящий документ ФСТЭК России 15.02.2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/289

4 Бурькова, Е.В. Задача оценки защищенности информационных систем персональных данных / Е.В. Бурькова, // Вестник Чувашского университета. - № 1, Чебоксары: ГОУ ВПО «ЧГУ».- 2016. - С. 112-118.

5 Коряков, Д. В. Разработка способа и устройства контроля изоляции в электрических сетях напряжением до 1кВ с глухозаземленной нейтралью.: автореф. дисс. ... канд. техн. наук / Д. В. Коряков. – Челябинск, 2005. –15 с.

6 Пат. 2 536 332 Российская Федерация, МПК G01R 27/00. Способ измерения сопротивлений изоляции присоединений и поиска присоединений с поврежденной изоляцией в сети постоянного тока с изолированной нейтралью / Галкин И. А., Иванов А. Б., Малышев А. Б, Лопатин А. А.; заявитель и патентообладатель Чебоксары. ООО научно-производ. предпр. «ЭКРА». – № 2013130130/28; заявл. 01.07.2013; опубл. 20.12.2014, Бюл. № 35. – 10 с.

7 Рахматуллин, Р.Р. Методические указания к расчетно-графическому заданию, курсовому и дипломному проектированию / Р.Р. Рахматуллин, Л.Ф. Давлетбаева. – Оренбург: ООО «Агентство «Пресса», 2008. – 29 с.

4.5 Проведение экспериментов и обработка результатов

Цель:

- апробация методики, разработанной в ходе выполнения задач ВКР;
- обработка результатов экспериментов;
- анализ полученных результатов.

В зависимости от индивидуального задания преддипломной практики данный этап будет состоять из различных видов выполняемых задач.

Если тематика ВКР связана с задачей модернизации существующей в организации системы защиты информации и других ресурсов, то возникает необходимость выбора средств защиты и рассмотрение вопроса об эффективности применения этих средств с точки зрения нейтрализации актуальных угроз безопасности информации [9, 20, 21, 25].

На основании построенной модели угроз проводится анализ вероятности нейтрализации актуальных угроз с использованием экспертного метода. В результате составляется таблица результатов по примеру таблицы 4.12.

Таблица 4.12 – Результаты анализа внедренных средств защиты

Внедренное средство или мера защиты	Актуальные угрозы	Вероятность реализации угроз
Сканер безопасности RedCheck	Недекларированные возможности в прикладном ПО	Низкая
	Непреднамеренная модификация информации сотрудниками	Низкая
	Установка ПО не для служебного пользования	Низкая
Доступ к содержанию электронного журнала возможен исключительно для должностных лиц	НСД к конфиденциальной информации сотрудников, не имеющих право доступа	Низкая
Межсетевой экран «Киберсейф: Межсетевой экран»,	Кража, модификация, уничтожение информации по сети	Низкая
McAfee Network Security M-4050 Sensor	Действия вредоносных программ	Низкая

Тематика ВКР, связанная с разработкой методов в области защиты информации подразумевают разработку программных продуктов. В этом случае на данном этапе необходимо провести апробацию работы разработанной программы в условиях предприятия (организации) прохождения преддипломной практики. Полученные результаты должны быть проанализированы и оформлены в виде представления интерфейсных окон с результатами работы программы, таблиц и графиков. Для проведения анализа необходимо использовать разработки авторов в области защиты информации [10, 11, 21, 25]. Пример показан на рисунке 4.7.

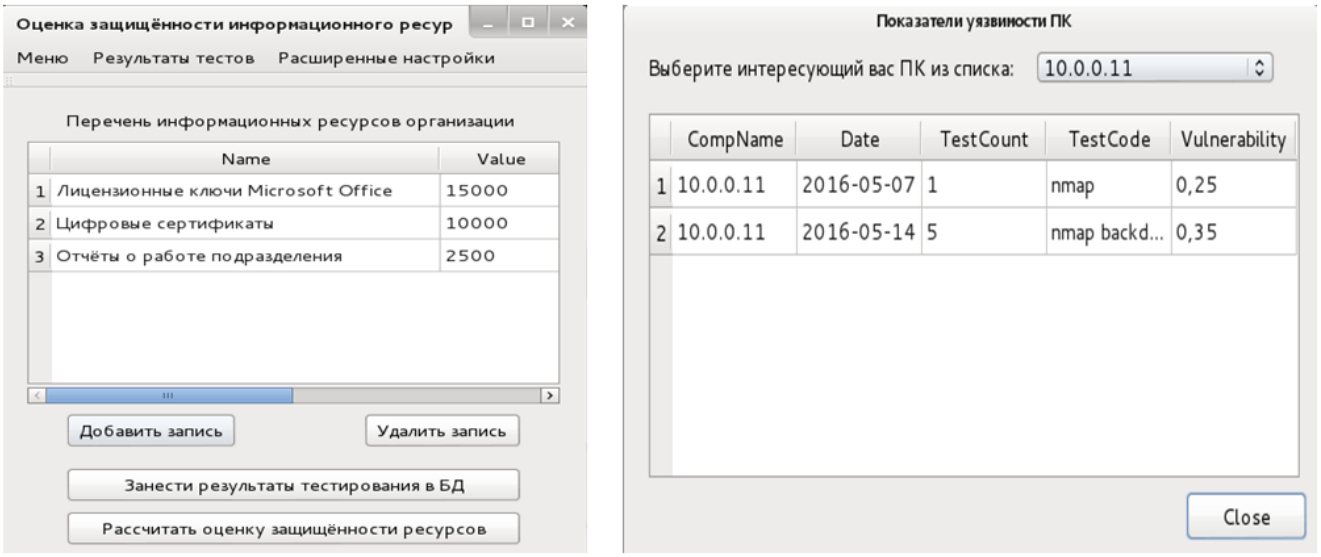
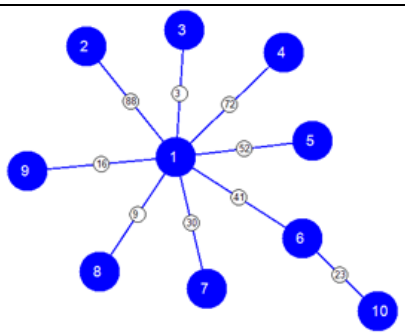
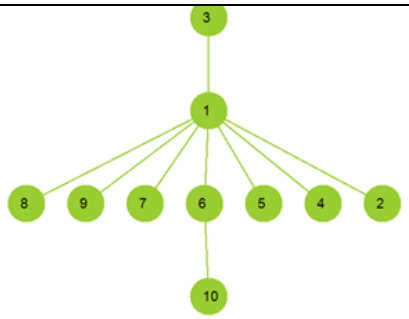
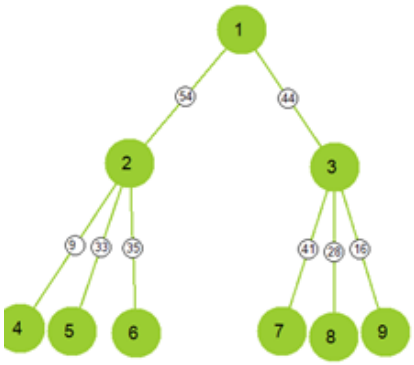
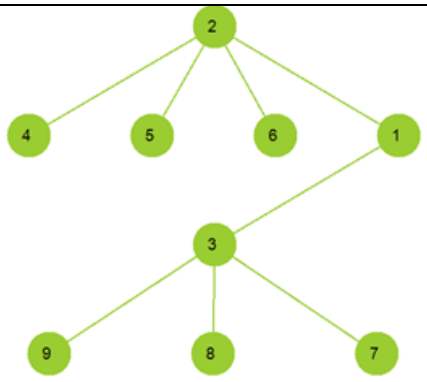


Рисунок 4.7 – Главное окно программы и окно результатов тестирования

Анализ результатов Может быть представлен в виде таблицы по примеру таблицы 4.13. В конце данного пункта необходимо сделать выводы о проделанных экспериментах и полученных результатах.

Таблица 4.13 – Сравнение результатов метода и модели прогнозирования маршрут распространения вредоносной программы

Топология сети	Маршрут распространения	Опасность заражения	
		S3	40
		S1	16
		S2	6.4
		S4	6.4
		S5	6.4
		S6	6.4
		S7	6.4
		S8	6.4
		S2	40
		S4	16
		S5	16
		S6	16
		S1	16
		S3	6.4
		S9	2.56
		S8	2.56
		S7	2.56

5 Составление и оформление отчета по практике

Цель:

- структурирование собранной информации по разделам;
- составление отчета по практике;
- оформление списка использованных источников;
- оформление дневника практики;
- сбор необходимых подписей и печатей предприятия.

Содержание отчета.

По окончании практики студент-практикант составляет письменный отчет и сдает его руководителю практики от университета одновременно с дневником, подписанным непосредственным руководителем практики от организации. По окончании практики студент не позднее семи дней после завершения практики сдает отчет комиссии, назначенной заведующим кафедрой.

Отчет должен содержать сведения о выполненной студентом работе в период практики. В отчете должна быть отражена фактически проделанная студентом работа с указанием методов выполнения, достигнутых результатов и выводов.

Отчет состоит из пояснительной записки объемом 30-35 страниц, где отражается содержание практики, и приложения, содержащие структурные, функциональные схемы, планы помещений объекта информатизации, принципиальные схемы компонентов автоматизированных систем обработки данных или ее подсистем, схемы алгоритмов, листинги программ, списка литературы по обзору предметной области индивидуального задания.

Основной текст содержания практики должен включать разделы:

- титульный лист;
- содержание;
- характеристика структуры и деятельности предприятия;
- постановка задач на выполнение индивидуального задания практики;

− обзор научно-технической литературы по теме индивидуального задания;

− анализ методов решения задачи по теме ВКР;

− анализ исходных данных информационной безопасности предприятия;

− модель нарушителя и модель угроз безопасности защищаемого объекта;

− концепцию решения поставленной задачи по теме ВКР;

− проведение экспериментов и обработка результатов;

− заключение, содержащее выводы по выполненным задачам;

− список использованных источников (не менее 30 пунктов);

− приложения (не менее 3).

К отчету прилагается:

− дневник;

− отзыв руководителя практики от предприятия о работе студента-практиканта.

Пример дневника практики приведен в таблице 4.14.

Таблица 4.14 – График выполненных работ

Дата	Описание работ	Подпись руководителя
1	2	3
9.04-10.04	Прохождение инструктажа по технике безопасности	
11.04-13.04	Сбор общей информации об организации. Сбор сведений, описывающих структуру и задачи, решаемые в организации	
16.04-18.04	Анализ характеристик технической укрепленности и радиоэлектронной обстановки выделенного помещения для проведения совещаний	

Продолжение таблицы 4.14

1	2	3
19.04-20.04	Анализ нормативно-правовой базы по защите конфиденциальной информации	
23.04-27.04	Разработка модели угроз и модели нарушителя для Департамента информационных технологий Оренбургской области	
30.04-4.05	Определение требований к системе защиты выделенного помещения для Департамента информационных технологий Оренбургской области	
7.04-10.05	Разработка обобщенной структурной схемы системы защиты выделенного помещения для проведения совещаний для Департамента информационных технологий Оренбургской области	
11.05-18.05	Выбор и обоснование технических средств и организационных мероприятий защиты выделенного помещения Департамента информационных технологий Оренбургской области	
21.05-25.05	Построение плана размещения технических средств системы защиты выделенного помещения Департамента информационных технологий Оренбургской области	
28.05-2.06	Составление и оформление отчета по практике	

Защита отчета по практике осуществляется в виде устного доклада и собеседования о проделанной работе и полученных результатах.

Список использованных источников

1 Артемов, А. В. Информационная безопасность курс лекций. [Электронный ресурс] А. В. Артемов – Орел: МАБИБ, 2014. – 257 с. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=428605

2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : Руководящий документ ФСТЭК России 15.02.2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/289

3 Буркова, Е. В. Категорирование объектов информатизации для выбора средств физической защиты / Е. В. Буркова // Материалы Всероссийской научно-метод. конф. «Университетский комплекс как региональный центр образования, науки и культуры». - Оренбургский гос. ун-т. – Оренбург: ООО ИПК «Университет», 2017. С. 3073-3076.

4 Буркова, Е. В. Профессиональная подготовка специалистов в области информационной безопасности [Электронный ресурс] / Буркова Е. В. // Вестник Оренбургского государственного университета,2016. - № 2. - С. 3-9.

5 Буркова, Е. В. Физическая защита объектов информатизации [Электронный ресурс]: учебное пособие / Е. В. Буркова - Оренбург: ОГУ, 2017. – 157 с.

6 Буркова, Е. В. Организация работ по защите персональных данных [Электронный ресурс]: учебное пособие / Е. В. Буркова - Оренбург: ОГУ, 2018. – 125 с.

7 Буркова, Е. В. Компьютерные технологии в образовании [Электронный ресурс]: методические указания / Е. В. Буркова – Оренбург: ОГУ, 2018. – 46 с.

8 Высшая аттестационная комиссия при Министерстве образования и науки Российской Федерации [Электронный ресурс]. – Режим доступа: http://vak.ed.gov.ru.

9 Галимов, Р. Р. Программно-аппаратные средства защиты информации в вычислительных системах [Электронный ресурс]: учебное пособие / Р. Р. Галимов, А. А. Рычкова - Оренбург : ОГУ. - 2017. - 132 с

10 Галимов, Р. Р. Управление информационной безопасностью [Электронный ресурс]: методические указания / Р. Р. Галимов, Е. И. Ряполова - Оренбург: ОГУ. - 2016. - 88 с

11 Кравцова, Е. Д. Логика и методология научных исследований: учебное пособие / Е. Д. Кравцова, А. Н. Городищева. – Красноярск: Сибирский федеральный университет, 2014. – 168 с.

12 Красильникова, В. А. Использование информационных и коммуникационных технологий в образовании / В.А. Красильникова. – Оренбург: ОГУ, 2012. – 292 с.

13 Мельников, В. П. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схитладзе; под ред. В. П. Мельникова. – М.: Академия, 2014. – 297 с.

14 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 14.02.2008 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380

15 Научная электронная библиотека elibrary.ru / [Электронный ресурс]. Режим доступа: https://elibrary.ru.

16 Об информации, информационных технологиях и о защите информации: Федеральный Закон от 26.07.07 № 149-ФЗ // Собрание законодательства Российской Федерации. – 2005. – 609 с.

17 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 №1119. [Электронный ресурс]. – Режим доступа: http://base.garant.ru/70252506/

18 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России № 21 от 18.02.2013 г. [Электронный ресурс]. – Режим доступа: http://base.garant.ru/70380924/

19 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России № 17 от 11 февраля 2013 г. [Электронный ресурс]. – Режим доступа: http://base.garant.ru/70391358/ .

20 Садердинов, А. А. Информационная безопасность предприятия: учеб. пособие для вузов / А. А. Садердинов, В. А. Трайнев, А. А. Федулов.- 2-е изд. - М.: Дашков и К, 2005. - 336 с.

21 Синилов, В. Г. Системы охранной, пожарной и пожарно-охранной сигнализации: учебник для нач. проф. образования / В. Г. Синилов. 6-е изд. — М. : Издательский центр «Академия», 2011. — 512 с.

22 Скрипник, Д. А. Общие вопросы технической защиты информации. [Электронный ресурс] / Д. А. Скрипник – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=429070

23 Стрельцов, А. А. Организационно-правовое обеспечение информационной безопасности: учебное пособие / А. А. Стрельцов, В. С. Горбатов, Т.А. Полякова. – М.: Издательский центр «Академия», 2008. - 256 с.

24 Хорев, П. Б. Программно-аппаратная защита информации: Учебное пособие / П. Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.