Министерство образования и науки Российской Федерации

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

Кафедра вычислительной техники и защиты информации

Е.В. Бурькова

ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рекомендовано к изданию Редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» в качестве методических указаний для студентов, обучающихся по программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2016

УДК 342.7
ББК 67.401 я7
Б 91

Рецензент – доктор технических наук, профессор В.И. Чепасов

Бурькова Е.В.

Б 91 Организация работ по защите персональных данных: методические указания к лабораторным работам / Е.В. Бурькова; – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2016. – 63 с.

В методических указаниях представлены основные этапы организации работ по защите персональных данных, сведения о составе и содержании мероприятий по обеспечению безопасности персональных данных объектов информатизации. Методические указания содержат материалы для проведения лабораторных работ по курсу «Организация работ по защите персональных данных», даны задания, вопросы для самопроверки.

Методические указания предназначены для студентов направления подготовки 10.03.01 Информационная безопасность.

УДК 342.7
ББК 67.401 я7

Содержание

Введение

Защита персональных данных является актуальной задачей, стоящей перед любой организацией, в которой обрабатываются сведения о работниках предприятия или сторонних лицах. В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» все организации обязаны обеспечить безопасность обрабатываемых персональных данных, причем реализовать меры защиты, соответствующие категории защищаемой информации и уровню защищенности информационных систем персональных данных.

Важной задачей является организация работ по защите персональных данных, создание комплекса мероприятий, включающего как организационные, так и технические меры защиты. Для реализации данной задачи разработан ряд нормативно-правовых документов, регламентирующих деятельность операторов персональных данных, устанавливающих требования к системе защиты обрабатываемых персональных данных, которые необходимо изучить и применять при проектировании системы защиты персональных данных в организациях.

Данные методические указания предназначены для проведения лабораторных работ по курсу «Организация работ по защите персональных данных» для студентов направления подготовки 10.03.01 Информационная безопасность. Методические указания содержат восемь разделов, в которых приведены теоретические сведения, даны задания и вопросы для самопроверки.

В процессе освоения данной дисциплины студенты приобретут знания нормативно-правовой основы защиты персональных данных, федеральных руководящих документов данной сферы, получат навыки построения модели угроз безопасности персональных данных, создания организационно-распорядительных документов и выбора технических средств защиты персональных данных.

Список сокращений и обозначений

АИС - Автоматизированная информационная система

АРМ - Автоматизированное рабочее место

АС - Автоматизированная система

АСЗИ - Автоматизированная система защищенного исполнения

БД - База данных

ГИС - Государственная информационная система

ИС - Информационная система

ИСПДн - Информационная система персональных данных

ИТ - Информационные технологии

КЗ - Контролируемая зона

НСД- Несанкционированный доступ

ПДн - Персональные данные

ПО - Программное обеспечение

ПЭМИН - Побочные электромагнитные излучения и наводки

СВТ - Средства вычислительной техники

СЗПДн - Система защиты персональных данных

СКЗИ - Средства криптографической защиты информации

СКХ - Сведения конфиденциального характера

СФ - Среда функционирования

СФК - Среда функционирования криптосредств

ТС - Техническое средство

УБПДн - Угрозы безопасности персональных данных

ЭП - Электронная подпись

1 Лабораторная работа № 1. Нормативно-правовая база защиты ПДн объекта информатизации

1.1 Цель работы

- Освоение основных понятий в области защиты ПДн;
- Изучение законодательных документов по защите ПДн.

1.2 Теоретические сведения

Во многих странах вопрос об обеспечении защиты персональных данных стал актуален намного раньше чем в России, именно поэтому институт защиты персональных данных на международном уровне является более развитым.

Одним из первых документов в данном вопросе является Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных», которая была утверждена 28 января 1981 г. в Страсбурге. Европейская конвенция рассматривает порядок сбора, хранения, способы физической защиты персональных данных, а также принципы доступа к таким данным.

Особое внимание в конвенции уделено требованиям, предъявляемым к персональным данным, проходящим автоматическую обработку. В частности предусмотрено, что персональные данные (далее - ПДн):

- должны быть получены и обработаны добросовестным и законным образом;

- должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;

- должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;

- должны быть точными и в случае необходимости обновляться;

- должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

Российская Федерация ратифицировала настоящую Конвенцию Федеральным законом от 19 декабря 2005 г. N 160-ФЗ, Конвенция вступила в силу для Российской Федерации 1 сентября 2013 г.

Определение понятия «персональные данные» дано в различных законодательных документах, оно отражает все признаки персональных данных и представлено в таблице 1.1.

Таблица 1.1 – Определение понятия «персональные данные»

Наименование нормативно-правового документа	Определение понятия «персональные данные»
ФЗ №152 «О персональных данных» от 27 июля 2006 г.	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
Конституция РФ	Информация, конкретно определяющая, идентифицирующая человека
Указ президента РФ № 188 от 6 марта 1997 года	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность
Трудовой кодекс РФ	Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника

Защита персональных данных – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранения и передачи персональных данных граждан. Комплекс мероприятий включает организационные и технические мероприятия. Организационные меры по защите персональных данных включают в себя: разработку организационно-распорядительных документов, которые регламентируют весь процесс получения,

обработки, хранения, передачи и защиты персональных данных; определение перечня мероприятий по защите ПДн. Технические меры по защите персональных данных предполагают использование программно - аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации, применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из класса системы персональных данных.

Защита ПДн и проектирование СЗПДн является актуальной задачей, стоящей перед любой организацией, в которой обрабатываются сведения о работниках предприятия и (или) о сторонних лицах.

При создании СЗПДн оператор (физическое или юридическое лицо, производящее обработку ПДн), руководствуется следующим перечнем документов.

1 Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

2 Федеральный закон Российской Федерации 30 декабря 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации (14 глава)».

3 Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4 Федеральный закон № 152-ФЗ «О персональных данных». В федеральном законе № 152-ФЗ даны общие понятия и определения в области защиты ПДн [8]. В этом законе изложены принципы обработки ПДн, обязанности оператора и права субъектов ПДн, требования к защите ПДн.

5 Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данным нормативно-правовым актом устанавливаются общие требования к доступу к ПДн [9].

6 «Специальные требования и рекомендация по технической защите конфиденциальной информации», утвержденные решением Коллегии Гостехкомиссии России от 2 февраля 2001 г. № 7.2 (далее – СТР-К). В СТР-К изложены поря-

док организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации [14].

СТР-К включает следующие вопросы защиты информации:

- организацию работ по защите информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при осуществлении переговоров;
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

7 Постановление Правительства РФ № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных, обрабатываемых в информационных системах персональных данных». В Постановлении даны определение категорий ПДн, уровней защищенности ПДн, требования к защите ПДн при их обработке в ИСПДн в соответствии с уровнями защищенности таких данных [11].

Необходимый набор мер в данном документе по защите ПДн отличается от ранее изданных документов, так, вместо классификации ИСПДн определяется уровень защищенности ИСПДн. Также в этом документе определяются угрозы трех типов, дана классификация ИСПДн в зависимости от категории обрабатываемых данных (специальные ИСПДн, ИСПДн, обрабатывающие биометрические ПДн, ИСПДн, обрабатывающие общедоступные ПДн и ИСПДн, обрабатывающие иные ПДн).

8 Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Данный приказ определяет необходимый набор требований к защите ПДн, обрабатываемых в ИСПДн, в зависимости от уровня защищенности [12].

9 Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Данный приказ определяет необходимый набор требований к защите ПДн, обрабатываемых в ГИС, в зависимости от уровня защищенности [13].

10 Руководящий документ ФСТЭК России 15.02.2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Этот документ содержит перечень угроз безопасности ПДн, обусловленных преднамеренными и непреднамеренными действиями субъектов. Классификация угроз проведена по таким признакам, как вид защищаемой информации, вид возможных источников угроз, тип ИСПДн, способ реализации угроз, вид нарушаемого свойства информации, используемые уязвимости и объект воздействия [2].

В результате применения описываемого документа решаются следующие задачи:

- разрабатываются частные модели угроз;
- проводится анализ защищенности ИСПДн от угроз;
- разрабатывается проект СЗПДн, направленной на нейтрализацию угроз;
- проводятся мероприятия по предотвращению несанкционированного доступа (далее – НСД);
- нейтрализуются воздействия на технические средства ИСПДн;
- контролируется обеспечение уровня защищенности ПДн.

8 Руководящий документ ФСТЭК России 14.02.2008 г. «Методика определения актуальных угроз безопасности персональных данных при обработке в информационной системе персональных данных».

Данная методика позволяет определить актуальные угрозы безопасности, применяя такие показатели как уровень исходной защищенности ИСПДн, вероятность реализации угрозы, опасность угрозы [5].

9 Указ Президента РФ от 22 мая 2015 г. N 260 «О некоторых вопросах информационной безопасности Российской Федерации». Порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет". Подключение информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" через российский государственный сегмент сети "Интернет" осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств (защищенные каналы). Федеральная служба охраны Российской Федерации (ФСО России) осуществляет контроль.

Согласно действующим документам в области защиты ПДн необходимо использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. Таким образом, для некоторых ИСПДн необходимо использовать сертифицированные средства защиты, а также проводить аттестацию ИСПДн.

1.3 Задание

1.3.1 Для заданного объекта информатизации изучить нормативно-правовые документы, регламентирующие защиту ПДн. Проанализировать какие виды тайн могут содержаться в обрабатываемых ПДн (врачебная тайна, коммерческая тайна, тайна личной жизни граждан). Найти нормативно-правовые документы, защищающие эти виды тайн в ПДн. Оформить результаты в виде таблицы.

1.3.2 Составить список всех персональных данных, обрабатываемых в данной организации, указать способ обработки ПДн, определить категорию ПДн.

1.3.3 По результатам выполнения пункта 1.3.1 составить таблицу по образцу таблицы 1.2. Количество строк таблицы варьируется в зависимости от объекта.

Таблица 1.2 - Нормативно-правовые документы по защите ПДн объекта

Наименование документа	Вид защищаемой информации	Краткие пояснения документа
Федеральные законодательные документы		
Внутренние документы организации		

1.4 Контрольные вопросы

1 Дать определение понятия «персональные данные» в соответствии с руководящими документами. Сформулировать определение категорий ПДн.

2 Какой нормативно-правовой документ является основополагающим для организации защиты ПДн? Дать характеристику разделов этого документа.

3 Что подразумевается под обработкой персональных данных? Сформулировать определения всех видов обработки ПДн. Кто проводит обработку ПДн?

4 Что входит в комплекс мероприятий по защите персональных данных? Привести описание видов мероприятий.

5 Какой нормативно-правовой документ устанавливает уровни защищенности ИСПДн? Привести краткое описание документа. Какие факторы влияют на уровень защищенности ИСПДн?

6 В чем отличие государственной информационной системы ПДн от других типов ИСПДн? Привести описание нормативных документов, регламентирующих требования по защите ПДн в таких ИС.

7 Каково назначение Руководящего документа ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при обработке в информационной системе персональных данных»?

2 Лабораторная работа № 2. Характеристика защищаемого объекта информатизации

2.1 Цель работы

- Исследование структуры и деятельности объекта информатизации;
- Анализ информационных ресурсов объекта, содержащих ПДн;
- Определение состава, категории и объемов обрабатываемых ПДн;
- Определение характеристик защищаемых ПДн.

2.2 Теоретические сведения

Обеспечение безопасности ПДн регламентируется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и направлено на решение следующих задач:

- предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- оперативное обнаружение фактов НСД к ПДн;
- предотвращение воздействия на технические средства автоматизированной обработки ПДн, приводящего к нарушению их функционирования;
- обеспечение быстрого восстановления ПДн, модифицированных или уничтоженных в результате НСД к ним;
- контроль за обеспечением безопасности ПДн в соответствии с уровнем защищенности ИСПДн.

Обязанности осуществления организационных и технических мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн возлагаются на оператора.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, под-

лежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общий порядок организации обеспечения безопасности ПДн включает:

- обследование объекта;
- обоснование требований по обеспечению безопасности ПДн и формулировку задача системы защиты;
- разработку концепции обеспечения безопасности ПДн;
- выбор мероприятий и средств защиты ПДн;
- реализацию мероприятий по обеспечению безопасности ПДн;
- контроль функционирования системы защиты ПДн.

Первый этап – это обследование объекта, в которое входит анализ информационных ресурсов объекта. В результате анализа определяется содержание и местонахождение ПДн, категорирование ПДн, оценка выполнения обязанностей по обеспечению безопасности ПДн. На этом же этапе определяют возможность физического доступа к ПДн, выявляют возможные технические каналы утечки, проводят анализ программно-математического воздействия на ПДн, анализ электромагнитного воздействия.

Важное место при обследовании объекта защиты ПДн уделяется оценке ущерба от реализации угроз безопасности и анализу имеющихся в распоряжении мер и средств защиты ПДн на объекте.

Характеристики безопасности персональных данных. Необходимо определить характеристики безопасности не только персональных данных, но и характеристики безопасности всех объектов, которые были определены как возможные объекты угроз.

Для ИСПДн определяют характеристики безопасности персональных данных, которые делятся на основные и дополнительные

Основные:

- конфиденциальность;
- целостность;
- доступность;

Дополнительные:

- неотказуемость;
- учетность (подконтрольность);
- аутентичность (достоверность);
- адекватность.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Доступность информации – состояние информации, при котором субъекты, имеющие права доступа могут реализовать их беспрепятственно.

2.3 Задание

2.3.1 Построить структурную схему отделов объекта информатизации. Привести краткое описание деятельности каждого отдела.

Привести перечень используемого программного обеспечения и средств вычислительной техники данного объекта, участвующих в обработке персональных данных. Пример перечня приведен в таблице 2.1.

Таблица 2.1 – Перечень ПО и технических средств объекта

Наименование	Месторасположение	Фирма-изготовитель
Программное обеспечение сервера		
Microsoft Windows Server 2008 R2	Сервер	Microsoft
Kaspersky Endpoint Security 10	Все ПК Организации	Лаборатория Касперского
1С: Бухгалтерия	ПК отдела «Бухгалтерия»	Назвать производителя
1С: Зарплата и кадры	ПК отдела кадров	Назвать производителя
Программное обеспечение АРМ информационных систем		
Microsoft Windows XP/ Vista/ 7	Перечислить кабинеты	Microsoft
Kaspersky Endpoint Security 10	Перечислить кабинеты	Лаборатория Касперского
Microsoft Office 2007/ 2010	Перечислить кабинеты	Microsoft
VipNet Client 3.2	Перечислить кабинеты	ОАО «Инфотекс»
Технические средства информационных систем		
Рабочие станции пользователей информационной системы	Кабинеты Организации	Назвать производителя
Сетевые кабели, соединяющие рабочие станции, сервер и модем	Помещения и коридор Организации	Назвать производителя
Кабели питания рабочих станций, обрабатывающих СКХ	Перечислить кабинеты	Назвать производителя
Линии вспомогательных средств и систем, размещенных в помещениях с техническими средствами, обрабатывающими СКХ	Перечислить кабинеты	Назвать производителя
Принтеры (локальные) и прочие печатающие устройства	Перечислить кабинеты	Назвать производителя
Система резервного питания	Перечислить кабинеты	Назвать производителя
Коммутатор сети	Перечислить кабинеты	Назвать производителя

2.3.2 Построить схему информационных потоков персональных данных объекта. Использовать сведения о деятельности и видах документов, циркулирующих между отделами организации. Создать табличное описание информационных потоков по примеру таблицы 2.2. Пример схемы информационных потоков отдела обслуживания читателей приведен на рисунке 2.1. на схеме можно обозначить номера потоков для их использования в табличном описании.

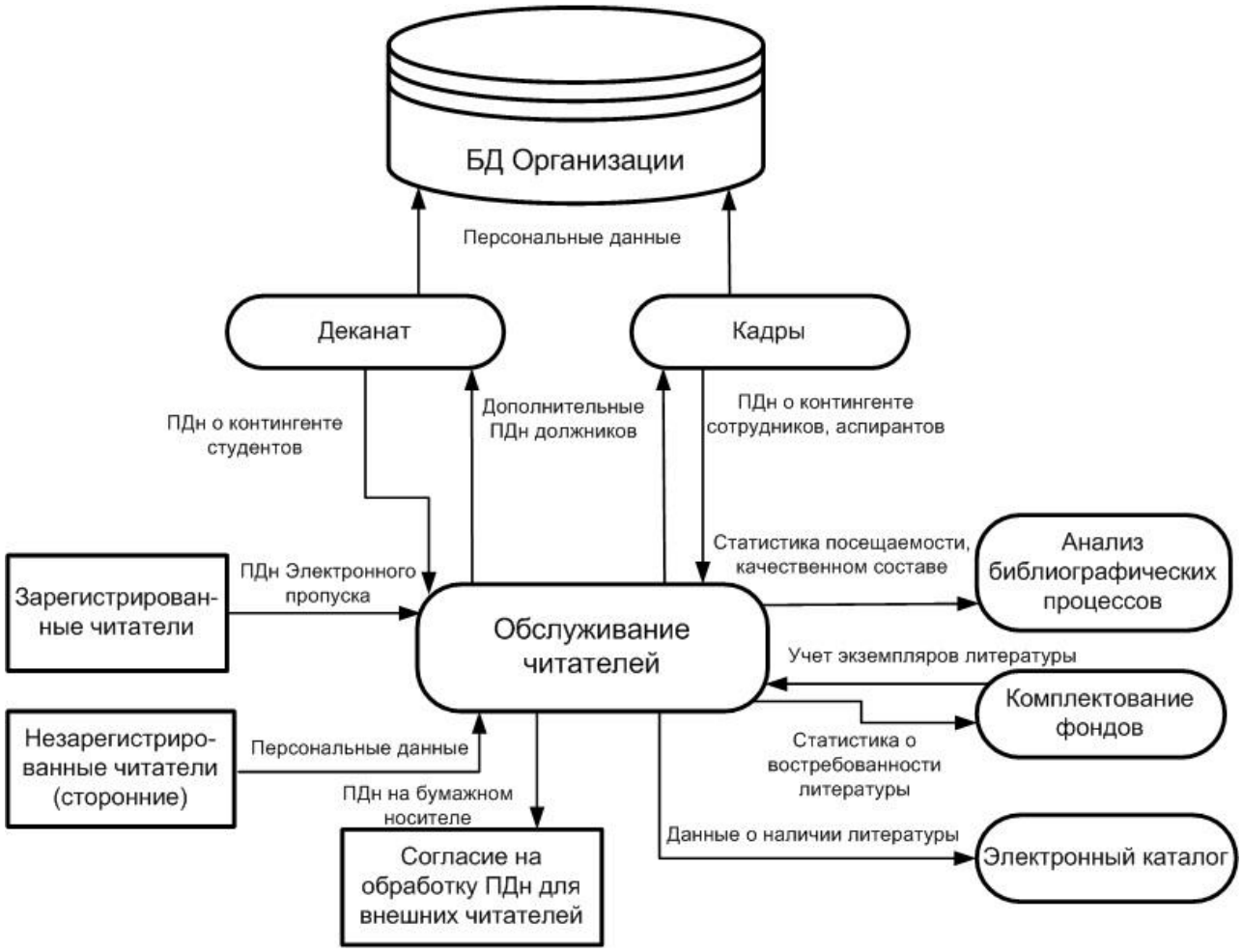

Рисунок 2.1 – Схема информационных потоков отдела обслуживания читателей

Таблица 2.2 – Табличное описание информационных потоков объекта

Номер информационного потока	Источник документа	Приемник документа	Содержание документа

2.3.3 Проанализировать ИСПДн, функционирующие на объекте. Привести текстовое описание каждой ИСПДн. Построить таблицу с результатами анализа, по примеру таблицы 2.3.

Таблица 2.3 – Анализ существующих ИСПДн объекта

Наименование ИСПДн	Краткое описание	Действия оператора ИПДн	Вид автоматизированной обработки
«Кадры»	Ведение личных дел сотрудников, записи в трудовые книжки, сведения о должностях и переводах в отделы Организации	ведется обработка персональных данных; заключение в письменной формы договоров	Автономные автоматизированные рабочие места операторов.
«Обслуживание клиентов»	Регистрация и обслуживание пользователей радиочастотным спектром – единая база сбора, учета и хранения данных о присвоенных радиочастотах.	ведется обработка персональных данных владельцев радиоэлектронных средств; требуется заключение письменной формы договора; оператор связи проверяет корректность предоставляемых абонентом данных для возможности информационного взаимодействия с ним.	Локальные вычислительные сети; распределенные вычислительные сети.

2.3.4 Определить состав, категории и объем обрабатываемых ПДн, источники и носители. Дать характеристику всех документов объекта, содержащих ПДн. Результаты занести в таблицу 2.4, в которой приведен пример заполнения.

Таблица 2.4 – Характеристика обрабатываемых ПДн объекта

Перечень ПДн	Источник ПДн	Объем ПДн	Вид носителя ПДн	Категория ПДн
Фамилия, имя, отчество, адрес места жительства, ИНН, паспортные данные, фотография, сведения о болезни	Трудовая книжка сотрудника, трудовой договор, личная карточка, больничные листы	< 100 000	Документы на бумажном носителе, жесткий диск компьютера	Иные, биометричекие, специальные, общедоступные

Определить группы обрабатываемых персональных данных в ИСПДн для различных уровней реализации служебных процессов: федеральный, региональный, муниципальный, местный. Могут быть группы трех типов:

1. Группа 1 – в ИСПДн находятся в процессе автоматизированной обработки персональные данные 100 000 и более либо данные субъектов в пределах субъекта Российской Федерации или Российской Федерации в целом;

2. Группа 2 – в ИСПДн находятся в процессе автоматизированной обработки персональные данные от 1000 до 100 000 субъектов ПДн либо данные субъектов, в пределах отрасли Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3. Группа 3 – в ИСПДн находятся в процессе автоматизированной обработки персональные данные менее 1000 субъектов ПДн или персональные данные субъектов ПДн, работающих в пределах конкретной организации.

2.3.5 Определить список требуемых характеристик безопасности персональных данных, обрабатываемых в информационных системах персональных данных на заданном объекте информатизации. Составить таблицу, отражающую способность ПО объекта реализовывать характеристики безопасности ПДн по примеру таблицы 2.4.

Таблица 2.4 - Характеристики безопасности ПО

Наименование программного обеспечения	Характеристика						
	Конфиденциальность	Целостность	Доступность	Неотказуемость	Учетность	Аутентичность	Адекватность
Microsoft Windows Server 2008 R2	-	+	+				
Kaspersky Endpoint Security 10	-	+	+				
Катарсис 7.57	+	+	+				
1С: Бухгалтерия	+	+	+				
АИС «Регистрация граждан»	+	+	+				

2.4 Контрольные вопросы

1 Дать характеристику основных задач системы защиты ПДн.

2 Что подразумевают под обработкой персональных данных? Дать определение всех действий, проводимых при обработке ПДн.

3 Назвать и охарактеризовать виды и способы обработки персональных данных. Что относят к автоматизированной обработке ПДн?

4 Дать определение всех категорий персональных данных, привести примеры. Указать законодательный документ, определяющий категории ПДн.

5 Дать определение оператора персональных данных, перечислить его основные обязанности.

6 Назвать и охарактеризовать принципы и условия обработки персональных данных.

7 Назвать основные права субъекта персональных данных.

8 Охарактеризовать особенности обработки специальной категории персональных данных.

9 Охарактеризовать особенности обработки биометрических персональных данных.

10 Перечислить меры по обеспечению безопасности персональных данных, согласно статьи 19 ФЗ-№ 152.

11 Дать определение основных и дополнительных характеристик безопасности персональных данных.

12 Перечислить и дать определения деструктивных действий в отношении ПДн, реализуемых при НСД к ним.

13 Каким образом осуществляется определение условий создания и использования персональных данных?

14 Дать определение понятия «распространение персональных данных».

15 Что такое трансграничная передача ПДн, какие предусмотрены требования при ее реализации.

3 Лабораторная работа № 3. Анализ характеристик информационных систем персональных данных объекта информатизации

3.1 Цель работы

- Определение форм фиксации персональных данных в ИС;
- Определение характеристик информационных систем персональных данных (ИСПДн) объекта;
- Определение показателей исходной защищенности ИСПДн объекта.

3.2 Теоретические сведения

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [8].

В соответствии с требованиями законодательства РФ безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Характеристика ИСПДн осуществляется на основе анализа исходных данных о системе и обрабатываемых в ней персональных данных. При проведении анализа ИСПДн необходимо учитывать следующие исходные данные:

– категория обрабатываемых в ИСПДн персональных данных;

– объем обрабатываемых в ИСПДн (персональные данные, находящие в ИСПДн в процессе автоматизированной обработки);

– заданные оператором характеристики безопасности персональных данных, обрабатываемых в ИСПДн.

Так как в данной лабораторной работе не анализируются угрозы безопасности ПДн, то и не может быть определен уровень защищенности ИСПДн в соответствии с Постановлением Правительства РФ № 1119. Этот уровень будет определен после построения модели угроз. Основные характеристики ИСПДн приведены в таблице 3.1.

Таблица 3.1 - Технические и эксплуатационные характеристики ИСПДн

Признак	Значение признака
По территориальному размещению	- распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; - городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); - корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; - локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; - локальная ИСПДн, развернутая в пределах одного здания.
По наличию соединения с сетями общего пользования	- ИСПДн, имеющая многоточечный выход в сеть общего пользования; - ИСПДн, имеющая одноточечный выход в сеть общего пользования; - ИСПДн, физически отделенная от сети общего пользования.
По встроенным (легальным) операциям с записями баз персональных данных	- чтение, поиск; - запись, удаление, сортировка; - модификация, передача.
По разграничению доступа к персональным данным	- ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн; - ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; - ИСПДн с открытым доступом.

Продолжение таблицы 3.1

По наличию соединений с другими базами ПДн иных ИСПДн	- интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); - ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн
По уровню обобщения (обезличивания) ПДн	- ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.); - ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; - ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)
По объему ПДн, которые предоставляются сторонним пользователям	- *ИСПДн без предварительной обработки:* - ИСПДн, предоставляющая всю базу данных с ПДн; - ИСПДн, предоставляющая часть ПДн; - ИСПДн, не предоставляющая никакой информации.
По наличию соединения с сетями международного информационного обмена (МИО)	- ИСПДн, подключенная к сетям МИО; - ИСПДн, неподключенная к сетям МИО.

Определение уровня исходной защищенности ИСПДн объекта. Согласно Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [5] исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений

по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент **Y1**:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Пример определения уровня исходной защищенности информационных систем приведен в таблице 3.2.

Таблица 3.2 - Уровень исходной защищенности информационных систем

Технические и эксплуатационные характеристики ИС	*Уровень защищенности*		
	Высокий	*Средний*	*Низкий*
1. По территориальному размещению			
Локальная автоматизированная система, развернутая в пределах одного здания	+	-	-
2. По наличию соединения с сетями общего пользования:			
Автоматизированная система, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с записями баз СКХ:			
Модификация, передача	-	-	+
4. По разграничению доступа к СКХ:			
Автоматизированная система, к которой имеют доступ определенные сотрудники организации, являющейся владельцем АС	-	+	-
5. По наличию соединений с другими базами СКХ иных ИС:			
Информационные системы, в которых используется по одной базе данных для каждой ИС, принадлежащих организации - владельцу данной ИС	+	-	-
6. По уровню обобщения (обезличивания) присутствующих ПДн:			
ИС, в которой предоставляемые пользователю персональные данные не являются обезличенными	-	-	+
7. По объему ПДн, предоставляемых сторонним пользователям:			
ИС, предоставляющая часть ПДн	-	+	-
Характеристики ИСПДн	***28,5%***	***43%***	***28,5%***

Данная ИСПДн имеет средний (**Y1=5**) уровень исходной защищенности.

3.3 Задание

3.3.1 Определить формы фиксации персональных данных (сведений конфиденциального характера (СКХ)) в информационных системах заданного объекта. Составить таблицу форм фиксации СКХ по образцу таблицы 3.3.

Таблица 3.3 - Формы фиксации СКХ

Формы фиксации	Обозначения
Резервные копии СКХ на съемном носителе	Фиксация_1
СКХ в виде сигналов в оперативной памяти технических средств	Фиксация_2
СКХ в областях (страницах) оперативной памяти	Фиксация_3
СКХ в виде сигналов передающихся через интерфейсы технических средств в открытом виде	Фиксация_4
СКХ в виде файлов (данных) на жестких магнитных дисках	Фиксация_5
Дополнить данными исследуемого объекта	

3.3.2 Определить технические и эксплуатационные характеристики ИСПДн заданного объекта. Для этого выписать из таблицы 3.1 необходимые данные, соответствующие ИСПДн исследуемого объекта.

3.3.3 Определить и обосновать тип ИСПДн объекта. Учесть, что государственные информационные системы зарегистрированы в Реестре Роскомнадзора. В ведении Роскомнадзора находится Единая информационная система (ЕИС Роскомнадзора), внесенная в реестр федеральных государственных информационных систем.

Согласно статье 13 Федерального закона N 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы включают в себя:

− государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основа-

нии соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (ГИС);

− муниципальные информационные системы, созданные на основании решения органа местного самоуправления (МИС);

− иные информационные системы.

Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

3.3.4 Определить уровень исходной защищенности ИСПДн объекта **Y1**, используя Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [5].

3.4 Контрольные вопросы

1 Дать определение информационной системы персональных данных, пояснить состав и назначение элементов ИСПДн.

2 Назвать и охарактеризовать технические и эксплуатационные характеристики ИСПДн.

3 Дать определения различных типов ИСПДн, описать их.

4 Какие нормативно-правовые документы применяют при разработке мероприятий по защите ПДн для различных типов ИСПДн? Дать краткую характеристику документов.

5 Назвать показатели исходной защищенности ИСПДн. Пояснить методику определения уровня исходной защищенности ИСПДн, указать руководящий документ.

6 Что такое формы фиксации СКХ, пояснить их назначение.

4 Лабораторная работа № 4. Анализ источников угроз и объектов воздействия угроз безопасности персональных данных

4.1 Цель работы

— Определение источников угроз безопасности ПДн объекта;

— Определение объектов воздействия угроз безопасности ПДн.

4.2 Теоретические сведения

Состав и содержание угроз безопасности персональных данных (УБПДн) в ИСПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным. Все множество источников УБПДн можно разделить на антропогенные (искусственные) и естественные. Естественные источники угроз включают техногенные и стихийные источники.

Стихийные источники угроз включают обстоятельства, составляющие непреодолимую силу, носящие объективный и абсолютный характер. К стихийным источникам относятся:

- природные катаклизмы;
- события социально-политического характера.

Техногенные источники угроз - это технические средства и технологии, которые могут выйти из-под контроля человека. Техногенные источники угроз могут быть как внешними, так и внутренними.

К техногенным источникам угроз относятся:

- средства связи;
- сети электропитания;
- системы кондиционирования;
- технические средства обработки информации;
- программное обеспечение (ПО).

Антропогенные источники - субъекты внутри или вне Организации, целенаправленные или ошибочные действия которых являются причиной нарушения безопасности ПДн. К ним относятся нарушители внешние и внутренние. Классификация угроз безопасности персональных данных представлена на рисунке 4.1.

Рисунок 4.1 - Классификация угроз безопасности персональных данных

Объекты воздействия угроз.

Информационные системы ПДн являются совокупностью информационных и программно-аппаратных элементов, средств вычислительной техники, применяемых при обработке ПДн.

Объектами воздействия угроз безопасности в ИСПДн являются:

− персональные данные, содержащиеся в базах данных;

− информационные технологии, применяемые при обработке ПДн;

− технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети,

средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее – технические средства ИСПДн);

− программные средства;

− средства защиты информации;

− вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, средства и системы охранной и пожарной сигнализации и другие [баз. модель].

Носитель информации – физическое лицо или материальный объект, а также физическое поле, в котором информация отображается в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПДн могут содержать информацию, представленную в следующих видах:

− акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн, а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

− видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в ИСПДн;

− информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

− информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

4.3 Задание

4.3.1 Определить источники угроз безопасности ПДн заданного объекта. Привести их текстовое описание и результаты оформить в виде таблицы по примеру таблицы 4.1.

Таблица 4.1 - Источники угроз безопасности ПДн

Вид источника угроз безопасности ПДн	Перечень источников угроз безопасности
Техногенные	средства связи
	сети электропитания
	системы кондиционирования
	технические средства обработки информации
	Продолжить по объекту
Антропогенные	внешние нарушители: *перечислить*
	внутренние нарушители: *перечислить*
Стихийные	Пожар, наводнение, взрыв газа

4.3.2 Определить объекты воздействия угроз безопасности ИСПДн. Привести их текстовое описание и результаты оформить в виде таблицы по примеру таблицы 4.2. Использовать Руководящий документ ФСТЭК России: Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [2].

Таблица 4.2 – Объекты воздействия угроз безопасности ИСПДн

Наименование объекта защиты	Местонахождение информации	Вид информации
Информация, обрабатываемая на АРМ ИСПДн	- на отчуждаемых носителях; - на жестких магнитных дисках; - на флеш-накопителях; - на аудио-, видеокассетах; - на встроенных носителях долговременного хранения; - в средствах обработки и хранения оперативной информации.	- защищаемые электронные документы в базах данных; - ключевая, аутентифицирующая и парольная информация
информационные технологии	*Заполнить по данным объекта*	*Заполнить по данным объекта*

Продолжение таблицы 4.2

Наименование объекта защиты	Местонахождение информации	Вид информации
технические средства, осуществляющие обработку ПДн	*Заполнить по данным объекта*	*Заполнить по данным объекта*
программные средства	*Заполнить по данным объекта*	*Заполнить по данным объекта*
Продолжить		*Заполнить по данным объекта*

4.3.3 Определить виды представления информации, содержащей ПДн, на данном объекте информатизации. Заполнить таблицу 4.3.

Таблица 4.3 – Виды и средства представления информации, содержащей персональные данные

Вид представления информации	Средства, содержащие ПДн
акустическая	*Заполнить по данным объекта*
видовая	*Заполнить по данным объекта*
информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур	*Заполнить по данным объекта*
Продолжить	*Заполнить по данным объекта*

4.3.4 Определить возможные способы нарушения характеристик безопасности персональных данных.

Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

− хищение персональных данных сотрудниками предприятия для использования в корыстных целях;

− передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;

− несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам предприятия;

− несанкционированное получение ПДн третьими лицами;

− уничтожение финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− модификация финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− блокирование финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− передача некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;

− искажение архивной информации по субъекту ПДн.

4.4 Контрольные вопросы

1 Дать определение понятия «источник угроз безопасности ПДн». На какие классы подразделяются все источники угроз безопасности ПДн?

2 Охарактеризовать антропогенные источники угроз безопасности ПДн. Привести перечень возможных внешних и внутренних нарушителей.

3 Дать характеристику внешних техногенных источников угроз безопасности ПДн.

4 Дать характеристику внутренних техногенных источников угроз безопасности ПДн.

5 Что такое программно-математическое воздействие на информацию? Кратко пояснить классификацию программно-математического воздействия.

6 Какие бывают виды и средства представления информации, содержащей персональные данные.

7 Описать объекты воздействия источников угроз безопасности ПДн.

8 Охарактеризовать способы нарушения характеристик безопасности персональных данных.

5 Лабораторная работа № 5. Построение модели нарушителя безопасности ПДн объекта

5.1 Цель работы

Определение характеристик внешнего и внутреннего нарушителей безопасности ПДн.

5.2 Теоретические сведения

В качестве субъектов атак (нарушителей) рассматриваются физические лица, имеющие доступ к техническим и программным средствам информационных систем.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все нарушители могут быть отнесены к следующим двум категориям:

− категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;

− категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

− внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ. В отношении

ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

− бывшие сотрудники предприятий отрасли;

− посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;

− представители преступных организаций.

Внешний нарушитель может осуществлять:

− перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

– деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

– несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;

– перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами;

– атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь категорий в зависимости от способа и полномочий доступа к информационным ресурсам ИСПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта.

К шестой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн. Лицо этой категории:

- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

− может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Привилегированные пользователи информационной системы, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства и СФК, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

5.3 Задание

5.3.1 Построить перечень внешних и внутренних нарушителей для данного объекта.

Определить характеристики и возможности внешних и внутренних нарушителей, каждому нарушителю присвоить порядковый номер HN, заполнить таблицы 5.1 и 5.2.

Таблица 5.1 – Характеристика внешних нарушителей объекта

Условное обозначение нарушителя	Наименование внешнего нарушителя	Характеристика внешнего нарушителя, возможные действия
Н1	Пользователи сетей связи общего пользования (злоумышленники)	Имеют высокую техническую квалификацию и знания о слабостях программных средств и сетевых протоколов. Могут реализовывать УБПДн из сетей связи общего пользования.
Н2	Уволенные сотрудники	В зависимости от прав доступа в ИСПДн, предоставленных при работе в Организации, могут обладать различными возможностями. Могут использовать для достижения своих целей знания о технологии работы, защитных мерах и правах доступа.
Н3…Н6	*Заполнить по заданному объекту*	*Заполнить по заданному объекту*

Таблица 5.2 – Характеристика внутренних нарушителей объекта

Условное обозначение нарушителя	Наименование	Описание	Возможности
Н7	Сотрудники	Сотрудники объекта, не имеющие доступа к ИСПДн	Имеют свободный доступ в КЗ объекта; могут получить ПДн видовой формы с экрана монитора, осуществить кражу паролей, кражу бумажных носителей ПДн.
Н8	Пользователи ИСПДн	Сотрудники, имеющие доступ к ПДн, обрабатываемым в ИСПДн объекта	Знают, по меньшей мере, одно легальное имя доступа. Обладают всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн. Располагают конфиденциальными данными, к которым имеет доступ.
Н9...НN	*Заполнить по заданному объекту*	*Заполнить по заданному объекту*	*Заполнить по заданному объекту*

5.3.2 Определить список субъектов, исключаемых из потенциальных нарушителей по примеру таблицы 5.3.

Таблица 5.3 - Субъекты, исключаемые из числа потенциальных нарушителей

Субъект	Обоснование
Инженеры - программисты	Инженеры-программисты не являются потенциальными нарушителями, так как заинтересованы в соблюдении характеристик безопасности защищаемых объектов в силу служебных обязанностей.
Администратор безопасности	Администратор безопасности не является потенциальным нарушителем, так как заинтересован в соблюдении характеристик безопасности защищаемых объектов в силу служебных обязанностей.
	Заполнить по заданному объекту

5.3.3 Построить таблицу об имеющейся у нарушителя информации по примеру таблицы 5.4.

Нарушители обладают полной информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты.

Таблица 5.4 - Информация, имеющаяся у нарушителя

Информация	Обозначения
Общие сведения об информационных системах, в которых используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационных систем)	Информация_1
Сведения об информационных технологиях, базах данных, ИС, ПО, используемых в информационной системе	Информация_2
Содержания находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ	Информация_3
Содержание технической документации на технические и программные компоненты СФК	Информация_4
Долговременные ключи криптосредства	Информация_5
Все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами	Информация_6
Сведения о физических мерах защиты объектов, в которых размещены СКЗИ	Информация_7
Сведения о линиях связи, по которым передается защищаемая информация	Информация_8
Все сети связи, работающие на едином ключе	Информация_9
Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК	Информация_10
Все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства	Информация_11
Сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства и СФК, которые может перехватить нарушитель	Информация_12
Сведения о мерах по обеспечению контролируемой зоны объектов информационной системы	Информация_13

Продолжение таблицы 5.4

Информация	Обозначения
Сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ	Информация_14
Общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ	Информация_15
Заполнить по заданному объекту	

5.3.4 Построить таблицу предположений об имеющихся у нарушителя средствах атак по образцу таблицы 5.5.

Нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, не составляющие государственную тайну.

Таблица 5.5 - Имеющиеся у нарушителя средства атаки

Средства атаки	Обозначение
Аппаратные компоненты криптосредства и СФК	Средтво_1
Доступные в свободной продаже технические средства	Средтво_2
Доступное в свободной продаже программное обеспечение	Средтво_3
Специально разработанные технические средства	Средтво_4
Специально разработанное программное обеспечение	Средтво_5
Штатные средства	Средтво_6
Заполнить по заданному объекту	

Ограничения на имеющиеся у нарушителей средства атак представлены в таблице 5.6.

Таблица 5.6 - Ограничения у нарушителя средств атаки

Субъект	Средтво_1	Средтво_2	Средтво_3	Средтво_4	Средтво_5	Средтво_6
Нарушитель_1	-	-	+	-	+	-
Нарушитель_3	+	-	-	-	-	+

Продолжение таблицы 5.6

Нарушитель_4	-	-	-	-	-	+
Нарушитель_6	-	-	-	-	-	-
Нарушитель_7	-	-	-	-	-	-
Заполнить по заданному объекту						

5.3.5 Построить таблицу соответствия нарушителей и их возможностей по образцу таблицы 5.7.

Таблица 5.7 - Соответствие нарушителей и их возможностей

Возможности нарушителя	Н1	Н3	Н4	Н6	Н7
Самостоятельное осуществление создания способов атак, подготовки и проведения атак	+	+	+	+	-
Действия на различных этапах жизненного цикла СКЗИ: - внесение несанкционированных изменений в СКЗИ и (или) в компоненты среды функционирования, в том числе с использованием вредоносных программ; - внесение несанкционированных изменений в документацию на СКЗИ и на компоненты СФ	+	+	+	+	-
Проведение атаки только извне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств	+	+	+	+	+
Проведение атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц	+	+	+	+	+
Заполнить по заданному объекту					

5.3.6 Построить результирующую модель нарушителя безопасности ПДн заданного объекта по образцу таблицы 5.8.

Таблица 5.8 - Модель нарушителя заданного объекта

Условное обозначение	Субъект безопасности ПДн	Категория	Тип нарушителя	Уровень технической подготовки	Уровень осведомленности
Н1	Конкуренты	I	Внешний	Средний	Низкий
Н2	Преступные организации	I	Внешний	Высокий	Средний
Н3	Легальные пользователи	II	Внутренний	Средний	Высокий
Заполнить	*Заполнить*	*Заполнить*	*Заполнить*	*Заполнить*	*Заполнить*

На основе анализа характеристик вероятных нарушителей, сделать вывод о категории нарушителя безопасности персональных данных заданного объекта.

5.4 Контрольные вопросы

1 Дать определение нарушителя безопасности ПДн. На какие типы подразделяются нарушители по наличию права постоянного или разового доступа в КЗ ИСПДн?

2 Перечислить всех возможных внешних нарушителей и их возможности.

3 Назвать и дать определение категорий внутреннего потенциального нарушителя в зависимости от способа доступа и полномочий доступа к ПДн.

4 Перечислить возможности внутреннего нарушителя I и II категорий.

5 Перечислить возможности внутреннего нарушителя III и IV категорий.

6 Перечислить возможности внутреннего нарушителя V и VI категорий.

7 Перечислить возможности внутреннего нарушителя VII и VIII категорий.

8 Что представляет собой модель нарушителя, дать характеристику основных учитываемых признаков.

9 На основании каких сведений определяется уровень технической подготовки и уровень осведомленности потенциального нарушителя?

7 Лабораторная работа № 6. Построение модели угроз безопасности ПДн объекта

6.1 Цель работы

— Провести анализ уязвимостей ИСПДн заданного объекта;

— Провести анализ угроз безопасности ПДн объекта;

— Определить актуальные угрозы безопасности ИСПДн.

5.2 Теоретические сведения

Угрозы безопасности персональных данных (УБПДн) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

− источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;

− среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

− носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, обра-

зов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Для реализации УБПДн источник угрозы может использовать уязвимости объектов воздействия и недостатки в организационных, технических и физических мероприятиях по обеспечению безопасности ПДн.

В соответствии с [2] и структурой ИСПДн защищаемого объекта выделяются следующие виды уязвимостей ИСПДн:

1) уязвимости подсистем ИСПДн;
2) уязвимости программного обеспечения (ПО):

– системного ПО;
– прикладного ПО;
– специального ПО;

3) уязвимости операционных систем:
   - в процессе инициализации ОС;
   - в незащищенном режиме работы процессора;
   - в процессе функционирования ОС;

4) уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств;
5) уязвимости СЗИ;
6) уязвимости, вызванные наличием программно-аппаратной закладки;
7) уязвимости, вызванные недостатками организационных, технических и физических мероприятий по обеспечению безопасности информации;
8) уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных;
9) уязвимости, вызванные недостатками организации ТЗИ от НСД;
10) наличие технических каналов утечки информации.

В таблице 6.1 приведена характеристика некоторых уязвимостей ИСПДн, которые могут быть использованы источником угрозы для реализации УБПДн.

Таблица 6.1 – Характеристика уязвимостей ИСПДн

Класс уязвимостей	Компоненты ИСПДн	Характеристика
Уязвимости подсистем ИСПДн	Подсистемы ИСПДн	Уязвимости данного класса связаны с НСД, с изменением или удалением информации, обрабатываемой в ИСПДн
Уязвимости ОС в процессе инициализации	Серверы ИСПДн, РС ИСПДн, СЗИ	Уязвимости данного класса связаны с нарушением штатного процесса загрузки ОС (например, загрузка сторонней ОС с внешнего носителя, изменение списка автоматически загружаемых программ, загрузка ОС в режиме восстановления)
Уязвимости ОС в процессе функционирования	Серверы ИСПДн, РС ИСПДн, СЗИ	Уязвимости данного класса вызываются ошибками в реализации ОС, использованием «слабых настроек безопасности» (отсутствие паролей, расширенные права пользователей, отсутствие экранных заставок, использование не стойких к подбору паролей), наличием известных критических уязвимостей и ошибками пользователей и администраторов ИСПДн
Уязвимости ПО, используемого для обработки ПДн	Серверы ИСПДн, РС ИСПДн	Уязвимости данного класса вызываются ошибками в реализации ПО, отсутствием поддержки со стороны производителей ПО и ошибками пользователей и администраторов ИСПДн
Уязвимости пользовательского ПО	РС ИСПДн, СЗИ	Уязвимости данного класса вызываются использованием пользователями ПО непроизводственного назначения на РС ИСПДн
Уязвимости протоколов сетевого взаимодействия	серверы ИСПДн, РС ИСПДн, СЗИ	Уязвимости данного класса, включают уязвимости в реализации протоколов сетевого взаимодействия (например, уязвимости в протоколах ARP, SMB)
Уязвимости, возникающие при передаче информации по каналам передачи данных	серверы ИСПДн, РС ИСПДн, СЗИ	Уязвимости данного класса включают случаи передачи информации по каналам передачи данных в открытом виде

Модель угроз для информационных систем персональных данных содержит систематизированный перечень угроз безопасности сведений конфиденциального характера при их обработке в информационных системах. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности сведений конфиденциального характера, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности сведений конфиденциального характера, обрабатываемых в информационных системах, связанным:

− с использованием средств криптографической защиты информации;

− с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

− с несанкционированным, в том числе случайным, доступом в ИС с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИС и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Анализ угроз безопасности сведений конфиденциального характера включает:

− описание угроз;

− оценку вероятности возникновения угроз;

− оценку реализуемости угроз;

− оценку опасности угроз;

− определение актуальности угроз.

Согласно [2] угрозы подразделяются на три типа, которые представлены в таблице 6.2.

Таблица 6.2 - Угрозы, представляющие потенциальную опасность для ПДн, обрабатываемых в ИСПДн

Угрозы
Угрозы 1 типа
Угроза наличия недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе
Угрозы 2 типа
Угроза наличия недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе
Угрозы 3 типа
Угрозы утечки акустической (речевой) информации
Угрозы утечки видовой информации
Угрозы утечки информации по каналам ПЭМИН
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на пере хват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.)
Угрозы внедрения вредоносных программ
Угрозы внедрения аппаратной закладки
Угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации
Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.
Угрозы выявления паролей
Угрозы получения НСД путем подмены доверенного объекта
Угрозы типа «Отказ в обслуживании»
Угрозы удаленного запуска приложений
Угрозы внедрения по сети вредоносных программ
Угрозы внедрения ложного объекта сети
Угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных
Угрозы уничтожения, хищения аппаратных средств ИС, носителей информации
Угрозы ошибочных действий пользователей
Угрозы ошибочных действий администратора безопасности

Продолжение таблицы 6.2

Угрозы
Угрозы ошибочных действий инженеров-программистов
Сбои в работе серверного и сетевого оборудования
Стихийные бедствия (пожары, затопление и т.д.)
Сбои в сети электропитания
Угроза пропуска инцидента информационной безопасности
Угроза невозможности своевременного обнаружения уязвимостей

Определение частоты реализации угроз безопасности ПДн.

Под частотой (вероятностью) реализации угрозы Y2 понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Частота реализации угроз безопасности ПДн определяется экспертным методом в соответствии с [5] и на основании результатов обследования ИСПДн.

Оценка вероятности реализации угрозы определяется по четырем вербальным градациям:

− маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);

− низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);

− средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (5);

− высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (10).

С учетом изложенного **коэффициент реализуемости угрозы Y** будет определяться соотношением

$$Y = (Y_1 + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

− если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

− если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы признается средней;

− если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы признается высокой;

− если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Определение опасности угроз безопасности ПДн.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования ИСПДн.

Показателем опасности, имеет три значения:

− низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

− средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

− высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Определение актуальных угроз безопасности СКХ.

Актуальная угроза - угроза, которая может быть реализована в ИС и представляет опасность для ПДн. Неактуальная угроза - угроза, которая не может быть реализована в ИС. Правила определения актуальности УБСКХ приведены в таблице 6.3.

Таблица 6.3 - Правила определения актуальности УБСКХ

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Далее составляется модель угроз в виде таблицы, в которой указаны все показатели. В таблице 6.4 приведен пример модели угроз безопасности ПДн.

Таблица 6.4 – Модель угроз безопасности ПДн

Угроза	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Показатель опасности угрозы	Актуальность угрозы
Угроза наличия недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Угроза наличия недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Угрозы утечки акустической (речевой) информации	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Угрозы утечки видовой информации	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Угроза НСД, реализуемая в ходе загрузки ОС	Средняя вероятность (5)	0,5 (средняя)	Высокая	Актуальная
Угроза НСД, реализуемая после загрузки ОС	Средняя вероятность (5)	0, 6 (средняя)	Высокая	Актуальная

Далее из таблицы составляют список актуальных угроз.

6.3 Задание

6.3.1 Провести анализ уязвимостей ИСПДн заданного объекта. Результаты записать в таблицу по образцу таблицы 6.1.

6.3.2 Проанализировать все вероятные угрозы безопасности ПДн заданного объекта и составить их перечень, используя таблицу 6.2.

6.3.3 Провести анализ частоты реализации угроз безопасности ПДн и опасности угроз. Построить модель угроз безопасности ПДн заданного объекта.

6.3.4 Определить перечень актуальных угроз ПДн заданного объекта. Сделать вывод о типе угроз, определить уровень защищенности ИСПДн объекта в соответствии с ПП № 1119.

6.4 Контрольные вопросы

1 Дать определение угрозы безопасности персональных данных.

2 Охарактеризовать основные элементы канала реализации УБПДн.

3 Что такое уязвимость ИСПДн, перечислить виды уязвимостей.

4 Дать характеристику уязвимостей ИСПДн.

5 Что подразумевают под частотой (вероятностью) реализации угрозы? Назовите вербальные градации этого показателя.

6 За счет чего быть реализованы угрозы безопасности ПДн?

7 Какие типы угроз существуют, перечислить угрозы 1 и 2 типов. Какой руководящий документ отражает типы угроз безопасности ПДн?

8 По какой формуле определяется коэффициент реализуемости угрозы, какова вербальная интерпретация реализуемости угрозы?

9 Каким образом оценивается опасность каждой угрозы?

10 Назовите правила отнесения угрозы безопасности ПДн к актуальной.

11 Как используют в дальнейшем список актуальных угроз безопасности ПДн?

12 Какими методами осуществляется выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств?

7 Лабораторная работа № 7. Обоснование требований по защите ПДн на объекте

7.1 Цель работы

Изучение порядка формирования требований по защите ПДн.

7.2 Теоретические сведения

Для формирования требований к защите ПДн необходимо использовать следующие руководящие документы:

− Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

− Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

− Приказ ФСТЭК России № 17 от 11 февраля 2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми

актами. При этом учитывается следующие факторы, какие ПДн обрабатываются в ИСПДн (специальные, биометрические и т.д.), учитывается объем обрабатываемых данных, отношение оператора, тип актуальных угроз. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных. И в зависимости от уровня защищенности ИСПДн устанавливаются требования к системе защиты ПДн [ПП 1119].

Состав и содержание мер по обеспечению безопасности персональных данных определяют приказы ФСТЭК № 21 и 17.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- Управление доступом субъектов доступа к объектам доступа (УПД);
- Ограничение программной среды (ОПС);
- Защита машинных носителей персональных данных;
- Регистрация событий безопасности (РСБ);
- Антивирусная защита (АВЗ);
- Обнаружение вторжений (СОВ);
- Контроль (анализ) защищенности персональных данных (АНЗ);
- Обеспечение целостности информационной системы и персональных данных (ОЦЛ);
- Обеспечение доступности персональных данных (ОДТ);
- Защита среды виртуализации (ЗСВ);
- Защита технических средств (ЗТС);
- Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);
- Выявление инцидентов и реагирование на них (ИНЦ);

− Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ).

Пример функций подсистем системы защиты ПДн приведен в таблице 7.1.

Таблица 7.1 – Функции подсистем системы защиты ПДн объекта

Подсистема защиты	Функции	Основания требований
1	2	3
Подсистема МЭ	− фильтрация на сетевом, прикладном и транспортном уровне; − фильтрация пакетов служебных протоколов; − регистрация и учет фильтруемых пакетов; − регистрация запуска программ и процессов; − регистрация, идентификация и аутентификация всех действий администратора МЭ; − содержать средства контроля за целостностью своей программной и информационной части; − восстановление после сбоев и отказов оборудования; − регистрация и учет запросов на установление виртуальных соединений; − возможность регламентного тестирования.	1. РД СВТ. МЭ Защита от НСД к информации Показатели защищенности от НСД к информации 2. Приказ ФСТЭК № 17
Подсистема управления доступом	− управление учетными записями, информационными потоками между устройствами; – разделение полномочий пользователей, администраторов; − ограничение неуспешных попыток входа в ИС; − реализация защищенного удаленного доступа.	Приказ ФСТЭК № 17
Подсистема регистрации и учета	− идентификация и аутентификация пользователей, устройств, объектов файловой системы; − управление идентификаторами, средствами аутентификации.	

Продолжение таблицы 7.1

1	2	3
Подсистема анализа защищенности	− выявление, анализ уязвимостей ИС и оперативное устранение уязвимостей; − контроль обновления ПО, включая ПО СЗИ; − контроль состава ТС, ПО и средств ЗИ.	
Подсистема обеспечения целостности	− контроль целостности ПО, включая ПО СЗИ; − восстановление ПО, включая ПО СЗИ; − защита от спама.	
Подсистема АЗ	− функции АЗ для класса 4А; − обновление базы данных признаков вредоносных компьютерных программ (вирусов); − централизованное управление подсистемой.	1. МД ИТ. САВЗ. А4. ПЗ 2. Приказ ФСТЭК № 17
Подсистема ОВ	− обнаружение вторжений для четвертого класса защиты; − централизованное управление подсистемой; − обновление базы решающих правил.	1. МД ИТ. СОВ. С4. ПЗ 2. Приказ ФСТЭК № 17

7.3 Задание

7.3.1 Учитывая уровень защищенности заданного объекта, определенный в лабораторной работе № 6, сформировать перечень требований к защите ПДн.

7.3.2 Записать классы требуемых средств защиты ПДН в зависимости от уровня защищенности ИСПДн объекта.

7.3.3 На основании сведений о том, к какому типу относится ИСПДн объекта, сформировать таблицу необходимых мер по защите ПДн, в соответствии с приказами ФСТЭК № 17 или № 21.

7.3.4 Составить структуру системы защиты ПДн объекта.

7.4 Контрольные вопросы

1 На основании каких данных устанавливаются требования к классу средств защиты ПДн? В каком документе определено это соответствие?

2 Каково содержание мер группы «идентификация и аутентификация субъектов доступа и объектов доступа»?

3 Каково содержание мер группы «управление доступом субъектов доступа к объектам доступа»?

4 Каково содержание мер группы «защита машинных носителей персональных данных»?

5 Перечислите содержание мер по защите ПДн в ГИС?

6 В чем различие мероприятий, устанавливаемых приказами ФСТЭК № 21 и № 17?

7 Как реализуется мера защиты «Обеспечение доступности персональных данных»?

8 В чем заключаются меры по защите технических средств?

9 В чем заключаются меры по защите информационной системы, ее средств, систем связи и передачи данных?

10 Какой орган выполняет работы по обеспечению безопасности персональных данных при их обработке в информационной системе?

11 Для защиты от каких действий принимаются меры по обеспечению безопасности персональных данных?

12 Кто проводит оценку эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных?

13 Что должны обеспечивать меры по выявлению инцидентов безопасности ПДн?

14 Что должны обеспечивать меры по антивирусной защите ПДн?

8 Лабораторная работа № 8. Выбор и обоснование технических средств защиты ПДн и организационных мероприятий на объекте

8.1 Цель работы

- Сформировать перечень средств защиты ПДн;
- Построить структурную схему системы защиты ПДн.

8.2 Теоретические сведения

На основании разработанной структуры системы защиты ПДн объекта формируют состав средств и мероприятий по защите ПДн объекта. А затем производят выбор технических и организационных мер в соответствии с требованиями руководящих документов к данному уровню защищенности ИСПДн.

В качестве примера рассмотрим систему защиты, состоящую из следующих подсистем:

- подсистема антивирусной защиты;
- подсистема межсетевого экранирования;
- подсистема обеспечения целостности;
- подсистема обнаружения вторжений;
- подсистема анализа защищенности.

В качестве защищаемой ИСПДн рассматривается ГИС второго уровня защищенности, характеристики приведены в таблице 8.1.

Таблица 8.1 – Характеристика ИСПДн

Название ИСПДн	Вид конфиденциальной информации	Количество субъектов	Назначение ИСПДн	Уровень защищенности ИСПДн
Государственная информационная система «Категории и льготы»	Специальная категория персональных данных	< 100000	Организация приема и обработки обращений от граждан, нуждающихся в помощи	2

Требования к защите ИСПДн приведены в таблице 8.2.

Таблица 8.2- Требования к защите ИСПДн

Уровень защи-	Класс защиты средств ЗИ					Уровень контроля ПО средств ЗИ на отсутствие НДВ
	СВТ	Средства антивирусной защиты	Системы обнаружения вторжений	Межсетевые экраны		
				Взаимодействие с сетями МИО	Отсутствие взаимодействия с сетями МИО	
2	Не ниже 5 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 уровня

Выбор конкретных средств защиты для выделенных подсистем проводится по результатам сравнительного анализа средств, который приведен в таблицах 8.3, 8.4.

Таблица 8.2- Сравнительный анализ и выбор средств МЭ

Наименование средства	Пропускная способность, Мб / сек	Количество допустимых сессий, тыс.	Память, Мб	Сетевые интерфейсы	Цена, тыс. руб	Маскировка портов	Восстановление работоспособности	Развертывание в Active Directory
Cisco PIX-515E	188	256	64	1 x RS-232, RJ-45; 2 x Ethernet 10Base-T/100 Base-TX, RJ-45	198	да	да	да
Juniper NetScreen 5GT	75	4	128	5 x 10/100 Ethernet 1 x 802.11 b/g	5	да	нет	да
Cisco PIX-506E	100	25	32	1 x RS-232, RJ-45; 2 x Ethernet 10Base-T/100 Base-TX, RJ-45	21	да	да	да
Cisco ASA 5520	450	280	512	4 x 10/100/1000 Gigabit Ethernet, 1 x 10/100 Fast Ethernet	60	да	да	да
Межсетевой экран Kerio Control	20	1	128	не предусмотрено	20	нет	нет	нет

Продолжение таблицы 8.3

Cisco 2621	15	5	256	4 x 10BaseT Ethernet	29	нет	нет	да
Cisco PIX-535	1000	500	512	10 x 10/100 Fast Ethernet или Gigabit Ethernet	561	да	да	да
Cisco ASA-5505	150	100	256	8 x RJ-45 10/100 Fast Ethernet с динамической группировкой портов	20	да	да	да

Таблица 8.2- Сравнительный анализ и выбор СОВ

Наименование средства	Пропускная способность, Мб / сек	Задержка, мкс	Количество одновременных соединений, тыс.	Сетевые интерфейсы	Цена, тыс. руб.	Режимы работы	Возможность кластеризации
Cisco IPS 4255	500	120	450	4 x Gigabit Ethernet	100	Сигнатурный	да
Cisco IDSM-2	600	120	600	8 x 10/100/1000 Fast Ethernet	129	Сигнатурный	нет
Juniper IDP 250	300	100	900	8 x 10/100/1000 Fast Ethernet	80	Комплексный	да
Juniper IDP 800	1000	100	700	10 x 10/100/1000 с режимом ByPass	660	Комплексный	да
IBM Proventia Network Intrusion Prevention System	200	100	1200	6 x 10/100/1000 Fast Ethernet	120	Эвристический	нет
Stone Gate IPS 1060	350	110	400	6 x 10/100/1000 Fast Ethernet	139	Эвристический	да

Таким же образом производят сравнение и выбор всех необходимых средств защиты ИСПДн. В результате формируют спецификацию выбранных средств защиты, представлена в таблице 8.3.

Таблица 8.3 - Спецификация средств защиты ИСПДн

Наименование средства	Фирма производитель	Примечание	Количество
Cisco ASA-5505	Cisco System	Межсетевой экран	1
Juniper IDP 250	Juniper Networks	Средство обнаружения вторжений	1
XSpider 7.8	Positive Technologies	Средство анализа защищенности	39
Dr.Web Enterprise Security Suite версия 10.0	ООО «Доктор Веб»	Средство антивирусной защиты	1
Acronis Backup	ООО «Акронис»	Средство резервного копирования	1

Строится структурная схема системы защиты ИСПДн объекта, пример схемы приведен на рисунке 8.1.

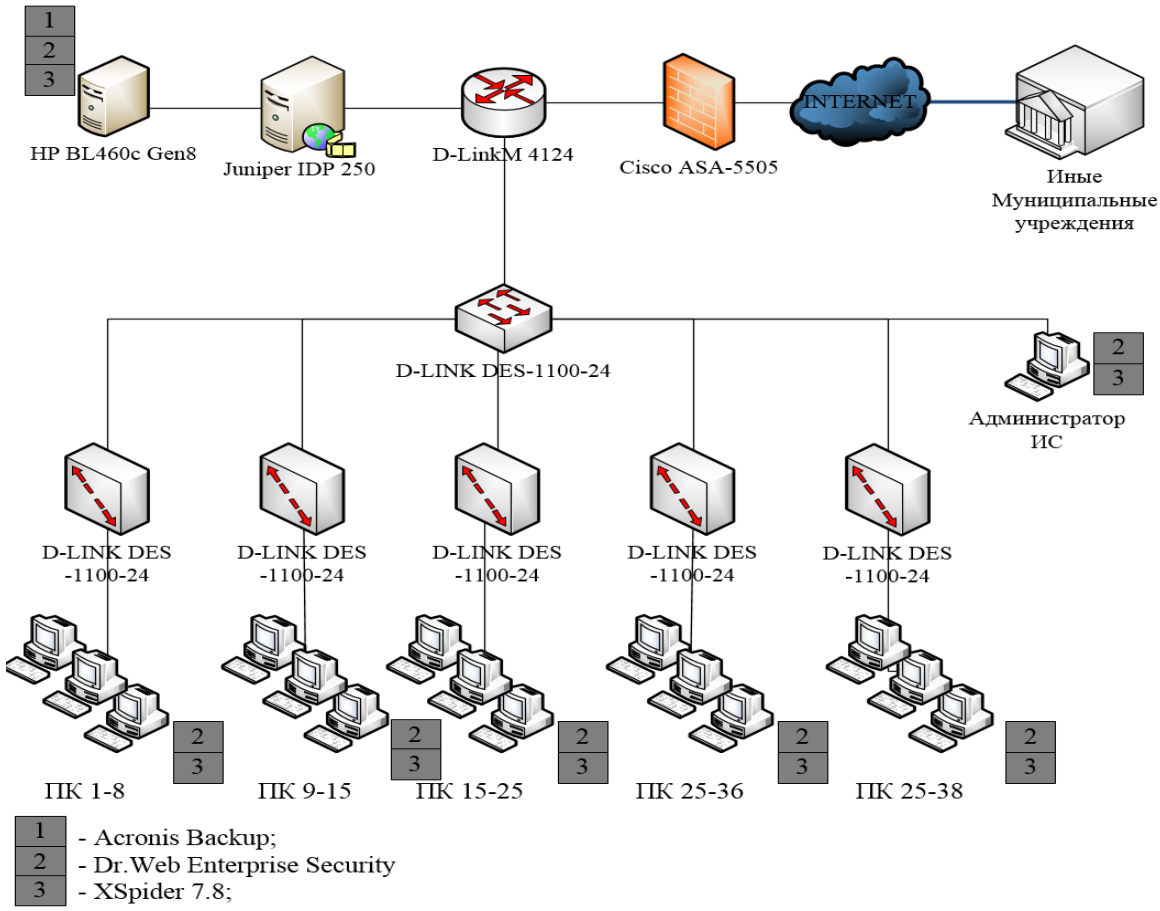

Рисунок 8.1 - Структурная схема системы защиты ИСПДн

В качестве организационных мероприятий по защите ПДн на объекте разрабатывают Инструкции по защите ПДн при автоматизированной обработке, Положение об обработке и защите персональных данных и другие документы. В таких документах подробно описан порядок обработки и защиты ПДн на объекте, перечень сотрудников, допущенных к ПДн, часто создается матрица доступа.

8.3 Задание

8.3.1 Занести в таблицы по примеру таблиц 8.1 и .8.2 характеристики и требования к средствам защиты ИСПДн. Создать список подсистем системы защиты ПДн объекта.

8.3.2 Провести сравнительный анализ и выбор средств защиты всех выбранных подсистем. Разработать спецификацию средств защиты ПДн.

8.3.3 Разработать структурную схему системы защиты ПДн объекта.

8.3.4 Разработать организационные меры по защите ПДн на объекте.

8.4 Контрольные вопросы

1 Дать обоснование критериев при осуществлении выбора средств защиты ИСПДн?

2 Назовите основные подсистемы, входящие в систему защиты ПДн. Дайте краткую характеристику.

3 Что подразумевается под средствами вычислительной техники для обработки ПДн и как определить их класс?

4 Назовите основные технические средства и организационные меры для реализации управления доступом субъектов доступа к объектам доступа.

5 Какими средствами реализуют защиту машинных носителей персональных данных?

6 Перечислите все функции, которые выполняют средства антивирусной защиты.

7 Какие организационные меры разрабатываются для обеспечения безопасности ПДн?

Список использованных источников

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

2 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : Руководящий документ ФСТЭК России 15.02.2008 г. – М. : ГТК РФ, 2008. – 55 с.

3 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.

4 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.

5 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 14.02.2008 г. – М. : ГТК РФ, 2008. – 73с.

6 Миронова, В.Г. Анализ этапов предпроектного обследования информационной системы персональных данных / В.Г.Миронова, А.А.Шелупанов // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. - 2011. - № 2 (35). - С. 45-48.

7 Назаров, И.Г. Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных / И.Г.Назаров, Ю.К.Язов, Е.С.Остроухова // Информация и безопасность. - 2009. Т. 12. - № 1. С. 71-76.

8 О персональных данных: Федеральный Закон от 27.07.2006 №152-ФЗ// Собрание законодательства Российской Федерации. – 2009. – 107 с.

9 Об информации, информационных технологиях и о защите информации: Федеральный Закон от 26.07.07 № 149-ФЗ // Собрание законодательства Российской Федерации. – 2005. – 609 с.
10 Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 15.02.2008 г. – М.: ГТК РФ, 2008. – 74с.
11 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 №1119 – 5 с.
12 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. – 20 с.
13 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России № 17 от 11 февраля 2013 г. – 23 с.
14 Специальные требования и рекомендация по технической защите конфиденциальной информации, утвержденные решением Коллегии Гостехкомиссии России от 2 февраля 2001 г. № 7.2.
15 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.
16 Шакирова, Р.А. Разработка алгоритма процесса проектирования частной модели угроз безопасности персональных данных / Р.А. Шакирова, Д.А. Заколдаев // Новый взгляд. Международный научный вестник. - 2015. - № 8. С. 165-168.