Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

А. В. Троеглазова

ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Утверждено редакционно-издательским советом университета
в качестве практикума для обучающихся по направлению подготовки
10.03.01 Информационная безопасность (уровень бакалавриата)

Новосибирск
СГУГиТ
2023

УДК 004.056:34
Т703

Рецензенты: кандидат юридических наук, доцент СибГУТИ *Е. А. Овчинникова*
кандидат технических наук, доцент, СГУГиТ *Д. Н. Титов*

Троеглазова, А. В.
Т703 Организационные и правовые основы информационной безопасности : практикум / А. В. Троеглазова. – Новосибирск : СГУГиТ, 2023. – 60 с. – Текст : непосредственный.
ISBN 978-5-907711-16-7

Практикум подготовлен Ph. D., доцентом А. В. Троеглазовой на кафедре информационной безопасности СГУГиТ.

В практикуме рассматриваются вопросы организации практических работ по дисциплине «Организационные и правовые основы информационной безопасности». Содержатся рекомендации по выполнению практических работ и контрольные вопросы для их защиты обучающимися по защите персональных данных.

Практикум по дисциплине «Организационные и правовые основы информационной безопасности» предназначен для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Рекомендован к изданию кафедрой информационной безопасности, Ученым советом Института оптики и технологий информационной безопасности СГУГиТ.

Печатается по решению редакционно-издательского совета СГУГиТ

УДК 004.056:34

ISBN 978-5-907711-16-7

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Основной *целью практикума* является формирование базовых компетенций и развитие у обучающихся способности анализировать нормативно-правовую документацию в сфере защиты персональных данных и использовать фундаментальные знания в процессе определения угроз безопасности информации при функционировании информационных систем персональных данных.

Задачи практикума – ознакомление обучающихся с основными законодательными и нормативными актами по сбору, обработке, хранению и защите персональных данных, этапами выявления угроз информационной безопасности при функционировании информационных систем персональных данных.

Настоящий практикум является руководством к выполнению двух практических работ по дисциплине «Организационные и правовые основы информационной безопасности» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата).

Описание каждой практической работы включает в себя цель работы, необходимое оборудование, длительность выполнения работы, порядок ее выполнения, форму отчета для представления результатов выполнения работы, контрольные вопросы для защиты практической работы. В начале каждой работы дан краткий теоретический материал, помогающий обучающемуся в осознанном выполнении заданий. Для более подробного изучения темы приведен библиографический список.

ОБЩИЕ ТРЕБОВАНИЯ К ОТЧЕТУ ПО ПРАКТИЧЕСКОЙ РАБОТЕ

Отчет по практической работе должен включать в себя следующие элементы:

1) ее номер;

2) название;

3) цель выполнения;

4) порядок выполнения;

5) результаты, полученные в ходе выполнения практической работы и представленные в виде таблиц, интеллект-карт;

6) подробный вывод по практической работе согласно поставленной цели.

Практическая работа № 1
ХАРАКТЕРИСТИКА ИНФОРМАЦИИ, ЗАЩИЩАЕМОЙ В ОРГАНИЗАЦИИ

Цель работы: провести анализ деятельности организации и сформировать перечень всех видов информации, защищаемых в данной организации.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Информацией называют сведения или данные, которые применяются во всех областях жизни человека независимо от формы их представления. Информацию классифицируют по различным признакам: по видам отражения (элементарная, биологическая, социальная, технико-кибернетическая), по связи с материальным носителем (свободная, связанная), по форме выражения (документированная и недокументированная), по роли в системе права (правовая, неправовая), по степени доступа (общедоступная и информация ограниченного доступа), по порядку распространения, по порядку предоставления и т. д.

В сфере информационной безопасности применяют классификацию информации по степени доступа к ней, при этом можно выделить два вида информации: общедоступная и информация ограниченного доступа. Общедоступной информация является либо по решению ее владельца, либо по требованию федеральных законов Российской Федерации. Так, законодательство РФ регламентирует открытый доступ ко всем нормативно-правовым актам о правах, свободах человека, полномочиях и деятельности государственных органов власти; к информации о состоянии окружающей среды; к информации об использовании государственными органами бюджетных средств; к информации в открытых фондах библиотек, архивов и т. п. Информация становится общедоступной при ее размещении в открытых источниках, например, в сети Интернет, в средствах массовой информации.

Информация ограниченного доступа может быть разделена на две группы: государственная тайна и конфиденциальная информация. К конфиденциальной информации согласно законодательству [1, 2] относится служебная тайна, персональные данные, коммерческая тайна, банковская тайна, прочие профессиональные тайны (врачебная, судопроизводства, следствия и т. д.), сведения о сущности изобретения. В зависимости от вида деятельности, выполняемых ею функций, статуса контрагентов в организации может осуществляться работа с различными видами информации.

Обладатель информации ограниченного доступа имеет право разрешать или ограничивать доступ к такой информации, определять порядок и условия такого доступа, использовать информацию и распространять ее по своему усмотрению, передавать информацию другим лицам по договору или на ином основании согласно законодательству, защищать свои права в случае незаконного получения информации или ее незаконного использования иными лицами, осуществлять иные действия с информацией или разрешать осуществление таких действий. При этом обладатель информации ограниченного доступа имеет следующие обязанности в отношении такой информации: предотвращать несанкционированный доступ к информации и/или передаче ее лицам, не имеющим соответствующих прав; осуществлять своевременное обнаружение фактов несанкционированного доступа к информации; предупреждать возникновение неблагоприятных последствий нарушения порядка доступа к информации; не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование; осуществлять незамедлительное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней; осуществлять непрерывный контроль за обеспечением уровня защищенности информации.

Классификация информации по уровню доступа регламентирована Федеральным законом «Об информации, информатизации и защите информации» № 149-ФЗ [2].

Порядок выполнения работы

1. Согласно заданию преподавателя (прил. 1) на основании данных, приведенных на сайте, изучить деятельность организации, привести словесное

описание характеристики организации (область деятельности, организационная структура) с указанием списка литературы, ссылок по тексту.

2. Учитывая область деятельности рассматриваемой организации, провести анализ исходных данных и предположить, какие виды информации могут обрабатываться в ней. Полученные результаты внести в табл. 1.1.

Отчет должен быть выполнен в тетради для практических работ (рукописно) и содержать следующие элементы:

1) номер и название практической работы;

2) цель выполнения практической работы;

3) формулировку задания с учетом варианта, распределенного преподавателем;

4) заполненная табл. 1.1;

5) итоговый вывод о проделанной работе.

Таблица 1.1

Результаты анализа информации, обрабатываемой в организации

№	Категории информации, обрабатываемой в организации	Тип данных, соответствующих категории
1		
2		
3		

Контрольные вопросы

1. Что называют информацией? Какие виды информации ограниченного доступа вы знаете? Приведите их характеристику.

2. Как проводить анализ деятельности организации для выявления категорий обрабатываемой информации?

Практическая работа № 2
АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ ДОКУМЕНТАЦИИ ПО ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ РЕЖИМА ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Цель работы: провести анализ нормативно-правовой документации по организации режима защиты государственной тайны.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Государственной тайной называют сведения в военной, внешнеполитической, экономической, разведывательной и контрразведывательной, оперативно-розыскной деятельности, при распространении которых может быть нанесен ущерб безопасности государства [2, 3]. Перечень сведений, составляющих государственную тайну [4, 5], представляет собой совокупность тех категорий сведений, в соответствии с которыми сведения относятся к государственной тайне. Засекречивание и рассекречивание таких сведений осуществляется на основаниях и в порядке, установленном федеральным законодательством РФ.

Перечень сведений, составляющих государственную тайну, регламентирован законодательными актами РФ [4], а меры ответственности за распространение сведений, составляющих государственную тайну, закреплены Уголовным кодексом РФ.

Для работы со сведениями, составляющими государственную тайну, и обеспечения процесса их защиты в организации создается режимно-структурное подразделение.

Носители информации, содержащие сведения, составляющие государственную тайну, могут быть отнесены к трем степеням секретности: особой важности, совершенно секретно, секретно. К сведениям особой важности относят информацию, разглашение которой наносит ущерб безопасности

государства; при нанесении ущерба министерству или отдельной отрасли экономики информацию относят к степени «совершенно секретно». В том случае, если при разглашении сведений наносится ущерб предприятию (организации), то считают, что такая информация имеет уровень доступа «секретно» [3].

Отнесение сведений к государственной тайне осуществляется руководителями государственных органов, имеющих на это право, согласно перечню должностных лиц, составленному межведомственной комиссией по защите государственной тайне и утвержденному Президентом РФ. На основании полученных данных межведомственная комиссия формирует единый перечень сведений, отнесенных к государственной тайне, который утверждается Президентом РФ и находится в открытом доступе [3].

К основным законодательным актам в сфере защиты государственной тайны можно отнести следующие:

– Федеральный закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ [6];

– Федеральный закон «Об информации, информатизации и защите информации» № 149-ФЗ [2];

– закон РФ «О государственной тайне» от 21.07.1993 № 5485-I [3];

– Указ Президента РФ от 11.02.2006 № 90 «О перечне сведений, отнесенных к государственной тайне» [4];

– Постановление Правительства РФ от 04.09.1995 № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» [5].

Система защиты государственной тайны включает в себя органы защиты государственной тайны, применяемые при этом средства и методы защиты, носители сведений, составляющих государственную тайну; мероприятия по защите государственной тайны.

Порядок выполнения работы

1. Изучите Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» [4].

2. Сформируйте перечень сведений, составляющих государственную тайну в зависимости от отрасли согласно заданию преподавателя (прил. 2). Полученные данные внесите в табл. 2.1.

Таблица 2.1

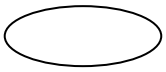
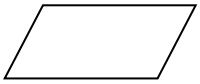
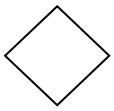
Перечень сведений, составляющих государственную тайну в отрасли

Сведения, составляющие государственную тайну	Государственный орган и организации, наделенные полномочиями по распоряжению сведениями	Наименование организаций Новосибирска и Новосибирской области

3. Составьте блок-схему, описывающую процесс организации и функционирования режима защиты государственной тайны в организации, учитывая условные обозначения, перечень которых представлен в табл. 2.2.

Таблица 2.2

Условные обозначения блок-схемы

Изображение	Обозначаемый алгоритм
	Начало или конец
	Ввод или вывод
	Принятие решения
	Дополнения действия

Отчет должен быть представлен в рукописном варианте в тетради для выполнения практических работ и содержать следующие элементы:

1) номер и название практической работы;

2) цель выполнения практической работы;

3) задание с учетом варианта, предоставленного преподавателем;

4) заполненная табл. 2.1;

5) вывод о проделанной работе.

Контрольные вопросы

1. Что называют государственной тайной? Какие грифы секретности вы знаете? Приведите их характеристику.

2. Какие законодательные и нормативно-правовые акты регламентируют процесс защиты сведений, составляющих государственную тайну?

3. С использованием составленной вами блок-схемы опишите процесс организации и функционирования режима защиты государственной тайны.

Практическая работа № 3
РАЗРАБОТКА КОМПЛЕКТА ДОКУМЕНТОВ ПО ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ РЕЖИМА ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

Цель работы: разработка комплекса организационно-распорядительных документов по защите коммерческой тайны на основании результатов анализа нормативно-правовой документации по организации режима защиты коммерческой тайны.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Коммерческой тайной называют один из видов конфиденциальной информации, разглашение которой может привести к снижению доходов организации и возникновению неизбежных расходов. Выделяют несколько видов коммерческой тайны: концептуальная, организационная, технологическая, параметрическая и эксплуатационная. К концептуальной коммерческой тайне можно отнести стратегию и концепцию развития организации, новые идеи в отношении создания и усовершенствования выпускаемой продукции. Организационная коммерческая тайна включает в себя список контрагентов, принимаемые управленческие решения, долгосрочные и краткосрочные планы производства. Технологическая коммерческая тайна отражает нововведения в технологическом процессе, ноу-хау, новые методы и технологии управления персоналом и финансами. К параметрической коммерческой тайне можно отнести любые числовые и расчетные сведения ограниченного доступа, утеря которых может привести к расходам организации. Эксплуатационная коммерческая тайна предполагает ограничение доступа к информации, касающейся эксплуатации и утилизации оборудования, любую информацию о системе защите в организации. К коммерческой тайне можно отнести базы данных клиентов и контрагентов

организации, содержание различных договоров, информацию о стратегии развития организации, ее ноу-хау, новых видах продукции и услуг, аутентификационную информацию, позволяющую ограничить доступ к коммерческой тайне, хранящейся в электронном виде; систему ценообразования организации, информацию о переговорах и порядке исполнения договоров и т. д. [2].

Доступ к коммерческой тайне могут иметь ее обладатели и правопреемники. Обладателями коммерческой тайны считаются как физические, так и юридические лица, которые осуществляют предпринимательскую деятельность и являются владельцами информации, составляющей коммерческую тайну. В качестве правопреемников можно считать и физических, и юридических лиц, которые на законном основании могут иметь доступ к коммерческой тайне. Такой юридической основой может быть выполнение ими должностных обязанностей, договор о передаче прав, право наследования. Обладатели коммерческой тайны обязаны соблюдать все права и интересы иных лиц, которых затрагивают данные сведения, принимать меры по защите информации, осуществлять реализацию режима защиты коммерческой тайны, ограничивать доступ к ней на основании требований законодательства. Режим защиты коммерческой тайны предполагает применение обладателем информации комплекса мер ее защиты с целью сохранения конфиденциальности, целостности и доступности коммерческой тайны. Организация режима состоит из нескольких этапов:

– установление перечня документов, относящихся к коммерческой тайне;

– документальное установление подробного порядка работы с коммерческой тайной;

– обеспечение строгого контроля и учета лиц, имеющих доступ к коммерческой тайне;

– нанесение на материальные носители грифа коммерческой тайны.

Порядок выполнения работы

1. Изучите законодательные и нормативно-правовые акты, регламентирующие процесс защиты коммерческой тайны.

2. Разработайте комплект документов по организации и функционированию режима защиты коммерческой тайны:

– форму акта об отказе работника дать письменные объяснения;

– акта об отказе работника ознакомиться с приказом;

– обязательства о соблюдении коммерческой тайны;

– приказа о наложении дисциплинарного взыскания;

– табеля учета лиц, имеющих допуск к коммерческой тайне;

– приказа о доступе к коммерческой тайне;

– положение о коммерческой тайне;

– положение о привлечении к дисциплинарной ответственности за нарушение режима коммерческой тайны.

Отчет о выполнении практической работы должен быть составлен в электронном виде (MS Word) и содержать комплект разработанных документов согласно заданию. Оформление документации должно соответствовать требованиям стандарта СТО СГУГиТ.

Контрольные вопросы

1. Что называют коммерческой тайной? Какие виды коммерческой тайны вы знаете? Приведите примеры.

2. Какие законодательные и нормативно-правовые акты регламентируют процесс защиты коммерческой тайны?

3. Опишите порядок организации режима коммерческой тайны на предприятии.

4. Приведите подробную характеристику мер защиты коммерческой тайны в организации.

Практическая работа № 4
АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Цель работы: проведение анализа нормативно-правовой документации по защите результатов интеллектуальной деятельности в Российской Федерации.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

К интеллектуальной собственности можно отнести результаты интеллектуальной деятельности организации, а также средства индивидуализации, в отношении которых осуществляется правовая охрана в соответствии с требованиями законодательных актов. В рамках защиты интеллектуальной собственности рассматривается авторское право и права, смежные с авторскими; патентное право, право на селекционное достижение, право на секрет производства (ноу-хау), права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий; право использования результатов интеллектуальной деятельности в составе единой технологии. Авторское право распространяется на произведения науки, литературы и искусства; программное обеспечение и базы данных. Авторское право возникает в момент создания объекта интеллектуальной собственности, оно является неотчуждаемым и неотделимым от личности автора. Авторские права являются бессрочными и передаются по наследству.

Патентное право применимо по отношению к изобретениям, полезным моделям и промышленным образцам. Субъектами патентного права являются автор и патентообладатель. При этом можно выделить три вида патентного права: личные неимущественные (авторское право), имущественные (исключительные) права и иные права.

Порядок выполнения работы

1. Изучите законодательные и нормативно-правовые акты, регламентирующие процесс защиты объектов интеллектуальной деятельности.

2. Составьте блок-схему с использованием уже известных вам обозначений (см. табл. 2.2) по алгоритму защиты объектов авторского права.

3. Составьте блок-схему с использованием уже известных вам обозначений (см. табл. 2.2) по алгоритму защиты объектов патентного права.

Контрольные вопросы

1. Дайте определение интеллектуальной собственности. Какие виды объектов интеллектуальной собственности вы знаете? Приведите примеры каждого из них.

2. Приведите основные этапы исторического развития интеллектуального права в России.

3. Какие объекты авторского и патентного прав вы знаете? Приведите их подробную характеристику и примеры.

4. Дайте определение понятию «признак объекта изобретения». Какие признаки вы можете назвать для таких объектов изобретений, как устройство, способ, вещество?

5. Приведите подробное описание с примерами прав различных субъектов – автора, заявителя и патентообладателя – при рассмотрении патентного права.

Практическая работа № 5
АНАЛИЗ ЭТАПОВ ИСТОРИЧЕСКОГО РАЗВИТИЯ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цель работы: проведение анализа основных этапов исторического развития системы защиты персональных данных в Российской Федерации.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Защита персональных данных (ПДн) в России началась еще в XIX в. В 1876 г. в период правления Александра II вступил в действие Почтовый устав, регламентировавший тайну корреспонденции. Ее нарушение, согласно Уголовному уложению, влекло за собой привлечение к уголовной ответственности. Начиная с 1903 г. и по 1917 г. к уголовной ответственности привлекали также должностных лиц в случае нарушения ими тайны личности. Сразу после проведения революции 1917 г. было отменено действие всех законодательных актов, регламентировавших тайну личности и тайну переписки. Официальное принятие нормативно-правовых актов о защите ПДн началось в 1950–60-х гг. с момента ратификации Пакта о гражданских и политических правах и разработки новой Конституции [7], регламентирующей права граждан на защиту ПДн. Законодательно запрет на сбор, хранение, использование и распространение информации о личности был введен в момент принятия Верховным Советом РСФСР в 1991 г. Декларации о неприкосновенности частной жизни. В 1995 г. ПДн были официально отнесены к конфиденциальной информации согласно принятому закону «Об информатизации и информации». Несмотря на принятие на территории стран СНГ в 1999 г. закона о защите ПДн, в России процедура защиты ПДн базировалась на европейской концепции [8], которая и легла в основу Федерального закона «О персональных данных» № 152-ФЗ [9]. Его особенности заключаются в рассмотрении ПДн в качестве самостоятельного

объекта права и разделении обязанностей между оператором и государством, которое выступает как надзорный орган.

Порядок выполнения работы

1. Изучить литературные данные (книги, монографии, научные статьи, учебные пособия и т. д.) по вопросу исторического развития информационной безопасности.

2. Составить инфографику по всем этапам исторического развития системы защиты персональных данных в мире и в Российской Федерации, определив названия и временные периоды каждого этапа исторического развития, особенности и исторических личностей каждого этапа. Обзор литературы подтвердить списком литературы, ссылками по тексту с указанием номера литературного источника и страницы размещения необходимой информации.

Отчет должен быть составлен рукописно в тетради для выполнения практических работ и содержать следующие элементы:

1) номер и название практической работы;

2) цель выполнения практической работы;

3) формулировку задания;

4) подробную инфографику, список литературы;

5) вывод о проделанной работе.

Контрольные вопросы

1. Приведите характеристику основных этапов развития процесса защиты ПДн.

2. Как бы вы охарактеризовали особенности современного этапа развития системы защиты ПДн в Российской Федерации?

3. Как развивалась система защиты ПДн в международном сообществе?

Практическая работа № 6
АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цель работы: проведение анализа нормативно-правовых актов РФ, регламентирующих процесс защиты персональных данных.

Оборудование: учебный персональный компьютер.

Время выполнения: 2 часа.

Общие теоретические сведения

Документально процесс защиты персональных данных в мире осуществляется с 1981 г. с принятия в Европе Конвенции «О защите личности в связи с автоматической обработкой персональных данных» [8], регламентирующей требования и условия процесса сбора, хранения, обработки и защиты ПДн в организациях различного уровня при условии их ручной и автоматической обработки. Конвенция устанавливает принципы процесса управления ПДн:

– добросовестность и законность получения и обработки;

– применение ПДн в случаях, не противоречащих действующему законодательству;

– адекватность и достаточность ПДн для достижения поставленных целей;

– точность и своевременная актуализация;

– хранение в форме, удобной для их идентификации и достаточной для достижения поставленных целей.

В России Конвенция Совета Европы [1] получила официальное признание лишь 1 сентября 2013 г. [10].

В законодательных и нормативно-правовых актах Российской Федерации приводятся различные определения термина «Персональные данные» [1, 7, 11], однако наиболее полное определение, отражающее требования законодательства в сфере защиты информации, представлено в федеральном законе № 152-ФЗ «О персональных данных» [9].

Под защитой персональных данных понимается разработка и реализация комплекса мероприятий в соответствии с требованиями нормативно-правовых актов Российской Федерации. Такие мероприятия условно подразделяют на три группы: правовые (законодательные), организационные и технические. Применение организационных мер защиты ПДн предполагает разработку, внедрение и поддержание в актуальном состоянии всего комплекса организационно-распорядительных документов, а также составление перечня мероприятий по защите ПДн. Важнейшим является применение для защиты ПДн программно-аппаратных средств (ПАС) защиты. Требования к применяемым средствам защиты информации – их количеству и классу, регламентированы рядом нормально-правовых актов. Защита ПДн и проектирование систем защиты персональных данных является актуальной задачей, стоящей перед любой организацией, в которой обрабатываются сведения о работниках предприятия и (или) о сторонних лицах.

При создании средств защиты ПДн оператор (физическое или юридическое лицо, производящее обработку ПДн) руководствуется следующим перечнем документов:

1) Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» [10];

2) Федеральным законом № 152-ФЗ «О персональных данных» [9]. В федеральном законе № 152-ФЗ даны общие понятия и определения в области защиты ПДн. В этом законе изложены принципы обработки ПДн, обязанности оператора и права субъектов ПДн, требования к защите ПДн;

3) Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» [1];

4) Федеральным законом Российской Федерации от 30.12.2001 № 197-ФЗ «Трудовой кодекс Российской Федерации» [11];

5) Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данным нормативно-правовым актом устанавливаются общие требования к доступу к ПДн [2];

6) специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утверждены решением Коллегии Гостехкомиссии России от 02.02.2001 № 7.2 (далее – СТР-К) [12].

СТР-К регламентирует подробный алгоритм проведения работ по технической защите конфиденциальной информации, включающей следующие вопросы:

– перечень и требования к содержанию всех видов документов в сфере технической защиты информации (организационно-распорядительной, проектно-технической и эксплуатационной документации);

– требования и рекомендации по защите речевой информации;

– 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 с применением различных типов средств вычислительной техники и информационных технологий;

– порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования;

7) Постановлением Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных, обрабатываемых в информационных системах персональных данных» [13].

В Постановлении приведены уровни защиты ПДн, регламентированы требования к порядку защиты ПДн при их обработке в информационной системе персональных данных (ИСПДн) в соответствии с установленным уровнем защиты, определены угрозы трех типов, описана классификация ИСПДн в зависимости от категории обрабатываемых данных (специальные ИСПДн; ИСПДн, обрабатывающие биометрические ПДн; ИСПДн, обрабатывающие общедоступные ПДн, и ИСПДн, обрабатывающие иные ПДн);

8) Приказом ФСТЭК России № 21 от 18.02.2013 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [14]. Документ регламентирует необходимый минимальный набор требований к защите ПДн, обрабатываемых в ИСПДн, в зависимости от ее уровня защищенности;

9) Приказом ФСТЭК России № 17 от 11.02.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах» [15]. Документ применяется только по отношению к ПДн, обрабатываемым в государственных информационных системах;

10) Руководящим документом ФСТЭК России от 15.02.2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [16].

Документ регламентирует перечень угроз безопасности ПДн в зависимости от вида защищаемой информации, возможных источников угроз, типа ИСПДн, способов реализации угроз, вида нарушаемого свойства информации, используемых уязвимостей ИСПДн и объекта воздействия. Применение основных положений руководящего документа позволяет разработать частную модель угроз, провести анализ защищенности ИСПДн от угроз, разработать проект средств защиты ПДн по нейтрализации угроз, применить мероприятия по предотвращению несанкционированного доступа, нейтрализовать воздействия на технические средства ИСПДн; осуществлять контроль обеспечения уровня защищенности ПДн;

11) Методическим документом ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации» [17].

Методика позволяет определить актуальные угрозы безопасности ПДн за счет применения уровня исходной защищенности ИСПДн, вероятности реализации угрозы, опасности угрозы.

Согласно действующим документам, в области защиты ПДн необходимо применять только сертифицированные средства защиты информации и проводить аттестацию ИСПДн.

Порядок выполнения работы

1. Изучите нормативно-правовые акты в сфере защиты персональных данных, перечень которых приведен в теоретической части работы.

2. Разработайте интеллект-карту для всех приведенных в п. 1 данной лабораторной работы нормативно-правовых актов. Интеллект-карта должна содержать четыре уровня:

– первый: наименование вида конфиденциальной информации – персональные данные;

– второй: обозначение нормативно-правового акта;

– третий: наименование направлений, рассмотренных в данном нормативно-правовом акте (не менее пяти наименований). При этом наименование направлений не обязательно должно соответствовать структуре документа. Название каждого направления должно быть представлено ассоциативно – слово или сочетание двух-трех слов;

– четвертый: для каждого раздела необходимо привести не менее пяти ассоциаций, характеризующих основную мысль, изложенную в данном разделе.

3. Воспользовавшись законодательными и нормативно-правовыми актами, проанализируйте меры ответственности, которые могут быть применимы за нарушение законодательства в области защиты персональных данных. Полученные данные внесите в табл. 6.1.

Таблица 6.1

Результаты анализа законодательных и нормативно-правовых актов по защите персональных данных в РФ

Вид ответственности	Наименование нормативно-правового документа	Статья	Мера ответственности

Отчет должен содержать следующую информацию:

1) номер и наименование практической работы, цель работы;

2) интеллект-карту, представленную в электронном формате или на бумажном носителе. Готовая интеллект-карта должна быть распечатана и вклеена в тетрадь для выполнения практических работ;

3) заполненную табл. 6.1;

4) вывод о проделанной практической работе.

Контрольные вопросы

1. Что называют персональными данными?

2. Какие виды персональных данных вы знаете? Приведите их подробную характеристику и примеры.

3. Дайте определения следующим понятиям: обезличивание ПДн, конфиденциальность ПДн, трансграничная передача ПДн, субъекты и операторы ПДн.

4. Каким образом в Российской Федерации осуществляется контроль и надзор за ПДн?

5. Приведите принципы процесса обработки ПДн.

Практическая работа № 7
РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цель работы: разработка комплекса организационных мер защиты персональных данных.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Процесс обработки ПДн осуществляется оператором ПДн, в качестве которого может выступать государственный или муниципальный орган, юридическое или физическое лицо, которое согласно требованиям законодательных актов обязано осуществлять защиту ПДн с применением организационных и технических мер. К организационным мерам защиты ПДн относятся следующие:

– назначение ответственного за организацию обработки ПДн;

– установление списка сотрудников, допущенных к процессу обработки ПДн;

– разработка политики по обработке ПДн;

– разработка локальных актов по вопросам, связанным с обработкой ПДн, их защитой и выявлением нарушений;

– обучение сотрудников организации с правилами сбора, хранения, обработки и защиты ПДн;

– составление перечня мероприятий по защите ПДн в организации;

– контроль выполнения требований законодательных и локальных актов к сбору, хранению, обработке и защите ПДн.

В организации-операторе по сбору и обработке ПДн разрабатываются общие и специализированные организационные меры по защите ПДн. К общим мерам можно отнести:

1) приказ об организации обработки ПДн;

2) положение по организации обработки и защите ПДн;

3) должностная инструкция лица, ответственного за организацию обработки ПДн;

4) проект приказа о перечне сотрудников, исполнение обязанностей которыми предполагает допуск к ПДн.

Положение об организации обработки и защите ПДн должно включать в себя следующие разделы:

– общие положения;

– состав и содержание ПДн организации;

– порядок сбора и обработки ПДн в организации;

– порядок передачи и хранения ПДн в организации;

– порядок организации и осуществления доступа к ПДн сотрудников организации и представителей государственных структур;

– меры ответственности сотрудников организации за нарушение требований по организации обработки и защите ПДн;

– права и обязанности сотрудников организации, ответственных за сбор, хранение и обработку ПДн;

– меры защиты ПДн, реализуемые в организации.

Положение об организации обработки и защите ПДн должно содержать подробное описание каждого раздела, формы организационно-распорядительных документов, перечень нормативно-правовых актов, список сокращений.

Должностная инструкция лица, ответственного за организацию обработки ПДн, должна включать в себя следующие разделы:

– общие положения;

– термины и определения;

– должностные права;

– должностные обязанности;

– действия ответственного при обнаружении попыток несанкционированного доступа к ПДн;

– меры ответственности.

Применение специализированных мер по защите ПДн предполагает разработку и применение следующих документов, перечень и общая

характеристика которых описаны в политике информационной безопасности ИСПДн:

1) план мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

2) план мероприятий по реализации контроля процесса обеспечения защиты ПДн;

3) порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;

4) должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

5) должностная инструкция администратора безопасности ИСПДн;

6) должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

7) инструкция на случай возникновения внештатной ситуации;

8) инструкция по размещению, оборудованию и охране помещений с ПДн.

План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн и план мероприятий по контролю обеспечения защиты ПДн включают общие положения и непосредственно планы мероприятий, представленные в табличной форме (табл. 7.1).

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации разрабатывается специалистом по защите ПДн (далее – Порядок) и утверждается первым руководителем организации. Порядок включает в себя следующие разделы:

– назначение и область применения;

– порядок реагирования на инциденты;

– организационные, физические и технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов в организации при защите ПДн.

Ответственность за обеспечение конфиденциальности, доступности и целостности ПДн несут администратор ИСПДн, администратор безопасности и пользователи ИСПДн, обязанности которых возлагаются приказом

руководителя организации на штатных сотрудников. Их права, обязанности, меры ответственности должны быть подробно и однозначно описаны в соответствующих должностных инструкциях. Каждая должностная инструкция разрабатывается ответственным лицом и утверждается первым руководителем организации под роспись в листе ознакомления назначенного штатного специалиста.

Таблица 7.1

Форма плана мероприятий

Мероприятие	Периодичность реализации	Должность ответственного лица
Организационные мероприятия		
Физические мероприятия		
Технические мероприятия		
Контролирующие мероприятия		

Инструкции, упомянутые в п. 7 и 8 данной практической работы, разрабатываются специалистом по информационной безопасности, утверждаются руководителем организации и вводятся в действие приказом руководителя о введении в действие документов системы менеджмента качества.

Инструкция на случай возникновения внештатной ситуации включает в себя следующие разделы:

– общие положения;

– действия работников в случае возникновения внештатных ситуаций;

– порядок проведения расследований при возникновении внештатных ситуаций;

– меры ответственности за возникновение внештатных ситуаций.

Инструкция по размещению, оборудованию и охране помещений с ПДн должна включать в себя:

– порядок доступа сотрудников организации и посетителей в помещения, в которых хранятся ПДн;

– организацию охраны и доступа в помещения с ПДн;

– требования к организационным, физическим и техническим мерам защиты ПДн в помещениях.

Порядок выполнения работы

Разработать общие организационные документы, регламентирующие процесс защиты ПДн:

– проект приказа об организации обработки ПДн в организации;

– положение по организации обработки ПДн;

– должностную инструкцию лица, ответственного за организацию обработки ПДн;

– проект приказа о перечне сотрудников, исполнение обязанностей которыми предполагает допуск к ПДн.

Отчет выполнения практической работы должен представлять собой комплект из четырех документов в электронном виде:

1) проект приказа об организации обработки ПДн в организации;

2) положение по организации обработки и защите ПДн;

3) должностную инструкцию лица, ответственного за организацию обработки ПДн;

4) проект приказа о перечне сотрудников, исполнение обязанностей которыми предполагает допуск к ПДн;

5) план мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

6) план мероприятий по контролю обеспечения защиты ПДн;

7) порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;

8) должностную инструкцию администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

9) должностную инструкцию администратора безопасности ИСПДн;

10) должностную инструкцию пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

11) инструкцию на случай возникновения внештатной ситуации;

12) инструкцию по размещению, оборудованию и охране помещений, где хранятся персональные данные, по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации.

Контрольные вопросы

1. Что называют персональными данными?

2. Какие виды персональных данных вы знаете? Приведите их подробную характеристику и примеры.

3. Дайте определения следующим понятиям: обезличивание ПДн, конфиденциальность ПДн, трансграничная передача ПДн, субъекты и операторы ПДн.

4. Каким образом в Российской Федерации осуществляется контроль и надзор за ПДн?

5. Приведите принципы процесса обработки ПДн.

Практическая работа № 8
ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН

Цель работы: определить уровень защищенности персональных данных, обрабатываемых в информационной системе персональных данных.

Оборудование: учебный персональный компьютер.

Время выполнения: 2 часа.

Общие теоретические сведения

Информационной системой является любая система, которая предназначена для работы и управления данными (сведениями). В литературе описаны различные типы информационных системы, классифицируемых по ряду признаков. В зависимости от характера информации, рассматриваемой в рамках определенной информационной системы, она может быть разделена на две основные группы: информационно-справочные системы и информационные системы обработки данных. В зависимости от объекта управления можно выделить системы управления ресурсами, предприятием, технологическими процессами, базами данных. Системы атоматизированного управления и системы автоматизированного проектирования занимают важное место среди информационных систем в рамках рассматриваемой классификации. В соответствии с положениями 149-ФЗ [2] можно выделить три вида информационных систем: государственные информационные системы (ГИС), муниципальные информационные системы (МИС) и иные информационные системы.

Те информационные системы, в которых осуществляется хранение и обработка ПДн с применением различных средств защиты информации, называются информационными системами персональных данных. Под ИСПДн понимают комплекс информационных и технических средств, содержащихся в базах данных, осуществляющих сбор, обработку и хранение ПДн.

Согласно положениям Постановления Правительства РФ от 01.11.2012 № 1119 [13] уровень защищенности ПДн при их обработке в ИСПДн определяется двумя факторами: типом угроз, актуальных для рассматриваемой ИСПДн, и категорией ПДн, обрабатываемых в рассматриваемой ИСПДн.

Выделяют три типа угроз, актуальных для ИСПДн, их характеристика представлена на рис. 8.1 [13].

Рис. 8.1. Типы угроз информационной безопасности

Тип угроз определяют путем анализа данных, полученных при обследовании ИСПДн организации.

Согласно требованиям законодательных актов [9, 13], можно выделить четыре категории ПДн: специальные, биометрические, общедоступные и иные. К специальным ПДн относится информация о расовой и национальной принадлежности субъекта, его политических, религиозных и философских взглядах, состоянии здоровья и т. д. Такие данные обрабатываются в ИСПДн-С. Биометрические ПДн связаны с физиологическими и поведенческими особенностями субъекта; такие данные (отпечатки пальцев,

радужная оболочка глаза и т. д.) обрабатываются в ИСПДн-Б. К общедоступным ПДн относятся любые данные, размещенные в общедоступных источниках (ФИО, дата и место рождения, номер телефона, домашний адрес, сведения об образовании и т. д.), но только с согласия субъекта на размещение таких данных. Такие ПДн обрабатываются в ИСПДн-О. К иным ПДн относятся все ПДн, не относящиеся к специальным, общедоступным и биометрическим категориям ПДн. Иные ПДн обрабатываются в ИСПДн-И.

В каждой из рассмотренных ИСПДн могут обрабатываться данные как сотрудников организации-оператора, так и лиц, не являющихся сотрудниками рассматриваемой организации.

После определения типа актуальных угроз и категории рассматриваемой ИСПДн с учетом количества субъектов обрабатываемых ПДн устанавливают уровень защищенности ИСПДн. Постановление Правительства РФ № 1119 [13] регламентирует четыре уровня защищенности ИСПДн, первый из которых является самым высоким, что обусловливает применение наиболее жестких мер по обеспечению защиты ИСПДн такого уровня.

Первый уровень защищенности устанавливают для ИСПДн, обрабатывающих специальные, биометрические и иные категории ПДн, для которых характерно наличие угроз 1-го типа. При наличии угроз 2-го типа первый уровень защищенности устанавливается для ИСПДн, обрабатывающей специальные данные при количестве субъектов более 100 тыс.

Второй уровень защищенности устанавливали в следующих случаях:

– при обработке в ИСПДн-С лиц, не являющихся работниками организации, количеством более и менее 100 тыс. для угроз третьего и второго типа соответственно, а также при обработке ПДн любого количества работников организации для угроз второго типа;

– при обработке в ИСПДн-Б работников и лиц, не являющихся работниками независимо от количества субъектов обрабатываемых ПДн при реализации угроз второго типа;

– при обработке в ИСПДн-И для лиц, не являющихся работниками организации, количеством более 100 тыс. субъектов для второго типа угроз;

– при обработке ИСПДн-О для лиц, не являющихся работниками организации, количеством более 100 тыс. субъектов – для первого и второго

типов угроз, менее 100 тыс. субъектов – для угроз первого типа, при обработке данных любого количества работников – для угроз первого типа.

Третий уровень защищенности устанавливают для следующих ИСПДн:

– ИСПДн-С при обработке данных не работников организации количеством менее 100 тыс. субъектов и любого количества работников организации при реализации третьего типа угроз;

– ИСПДн-Б при обработке любого количества данных не работников организации и любого количества работников организации при реализации третьего типа угроз;

– ИСПДн-И при обработке любого количества данных не работников организации при реализации третьего и второго типов угроз соответственно, любого количества работников организации при реализации угроз второго типа;

– ИСПДн-О при обработке данных не работников организации менее 100 тыс. и любого количества работников организации при реализации второго типа угроз.

Четвертый уровень защищенности устанавливают для следующих ИСПДн:

– ИСПДн-И при обработке данных не работников организации количеством менее 100 тыс. субъектов и любого количества работников организации при реализации третьего типа угроз;

– ИСПДн-О при обработке любого количества данных не работников организации и любого количества работников организации при реализации третьего типа угроз.

Порядок выполнения работы

1. Проведите анализ исходных данных согласно заданию (варианты распределяются преподавателем на основании прил. 3), установите категорию обрабатываемых ПДн (табл. 8.1).

В зависимости от типа информационной системы, категории и количества субъектов ПДн определите уровень защищенности информационной системы.

Таблица 8.1

Перечень ПДн, обрабатываемых в ИСПДн

Содержание ПДн	Цели обработки ПДн	Основание для обработки ПДн	Количество обрабатываемых субъектов ПДн	Категория ПДн	Вид обработки

Отчет должен быть составлен рукописно в тетради для выполнения практических работ и содержать следующие элементы:

1) номер и название практической работы;

2) цель практической работы;

3) задание, выданное преподавателем, вариант;

4) заполненную табл. 8.1;

5) вывод о проделанной практической работе.

Контрольные вопросы

1. Что называют информационной системой? Какие виды информационных систем вы знаете? Приведите их примеры.

2. Какие категории персональных данных вам знакомы? Приведите характеристику перечисленных категорий персональных данных.

3. Что называют уровнем защищенности? Какие нормативно-правовые акты РФ регламентируют процесс определения уровня защищенности ПДн, обрабатываемых в ИСПДн?

4. Опишите подробный алгоритм установления уровня защищенности персональных данных, обрабатываемых в ИСПДн.

Практическая работа № 9
ОПРЕДЕЛЕНИЕ ПЕРЕЧНЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цель работы: установить перечень актуальных угроз безопасности персональных данных в организации.

Оборудование: учебный персональный компьютер.

Время выполнения: 4 часа.

Общие теоретические сведения

Под угрозами безопасности ПДн понимают комплекс условий и факторов, которые реализуют опасность нарушения доступности, конфиденциальности и целостности ПДн при их обработке в ИСПДн вследствие случайного или преднамеренного несанкционированного доступа со стороны работников организации и сторонних лиц.

Согласно положениям Постановления Правительства РФ от 01.11.2012 № 1119 [13] меры по обеспечению безопасности персональных данных должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных. Поэтому обязательным этапом построения системы защиты персональных данных в информационной системе персональных данных организации является определение актуальных угроз безопасности согласно требованиям методики оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021 [17].

При проведении оценки угроз безопасности информации специалистами по информационной безопасности должны быть решены задачи, перечень которых представлен в виде ассоциативного ряда на рис. 9.1 [17].

Порядок оценки угроз безопасности информации включает в себя три основных этапа, представленных на рис. 9.2.

Реализацию этапов 1, 3.1 и 3.3 согласно требованиям методики [17] рекомендуется проводить экспертным методом.

Рис. 9.1. Ассоциативная схема задач процесса оценки угроз безопасности информации

Рис. 9.2. Этапы процесса определения угроз безопасности информации

При выполнении первого этапа экспертами проводится анализ возможных негативных последствий, которые могут быть реализованы при функционировании ИСПДн в организации и нанести ущерб как личности, так и организации в целом. К таким последствиям можно отнести следующие: нарушение приватности личной и семейной жизни, утрата репутации и доверия, принятие ошибочных решений, нарушение работоспособности информационной системы или сети, распространение ложной информации организации на веб-ресурсах, несанкционированный доступ к системам и сетям с целью злоупотребления вычислительными мощностями, использование государственных веб-ресурсов для распространения и управления вредоносным программным обеспечением, утечка ограниченной информации.

На втором этапе путем анализа исходных данных устанавливаются объекты воздействия, перечень которых представлен на рис. 9.3.

Рис. 9.3. Список объектов воздействия при реализации угроз [17]

Третий этап предполагает выполнение следующих видов работ [17]:

– 3.1: определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

– 3.2: оценка способов реализации (возникновения) угроз безопасности информации;

– 3.3: оценка сценариев реализации угроз безопасности информации в системах и сетях.

Определение источников угроз (этап 3.1) предполагает установление категории нарушителей (внутренние или внешние) и их потенциала (низкий, средний, высокий). Для этого экспертным методом устанавливают перечень актуальных нарушителей из общего списка на основе анализа исходных данных для рассматриваемой ИСПДн (рис. 9.4).

Для установленного перечня актуальных нарушителей и их категорий на основании данных прил. 8 методики [17] оценивают уровень возможностей каждого нарушителя. Далее необходимо найти соответствие уровня возможностей и потенциала нарушителей согласно данным табл. 9.1.

Этап 3.2 предполагает выбор из установленного перечня всех возможных способов реализации (возникновения) угроз безопасности информации. Краткий перечень таких способов представлен на рис. 9.5.

Таблица 9.1

Сведения о нарушителях [17]

Уровень возможностей	Потенциал нарушителей
Высокий (Н4)	Высокий
Средний (Н3)	Средний
Базовый с повышенными возможностями (Н2)	
Базовый (Н1)	Низкий

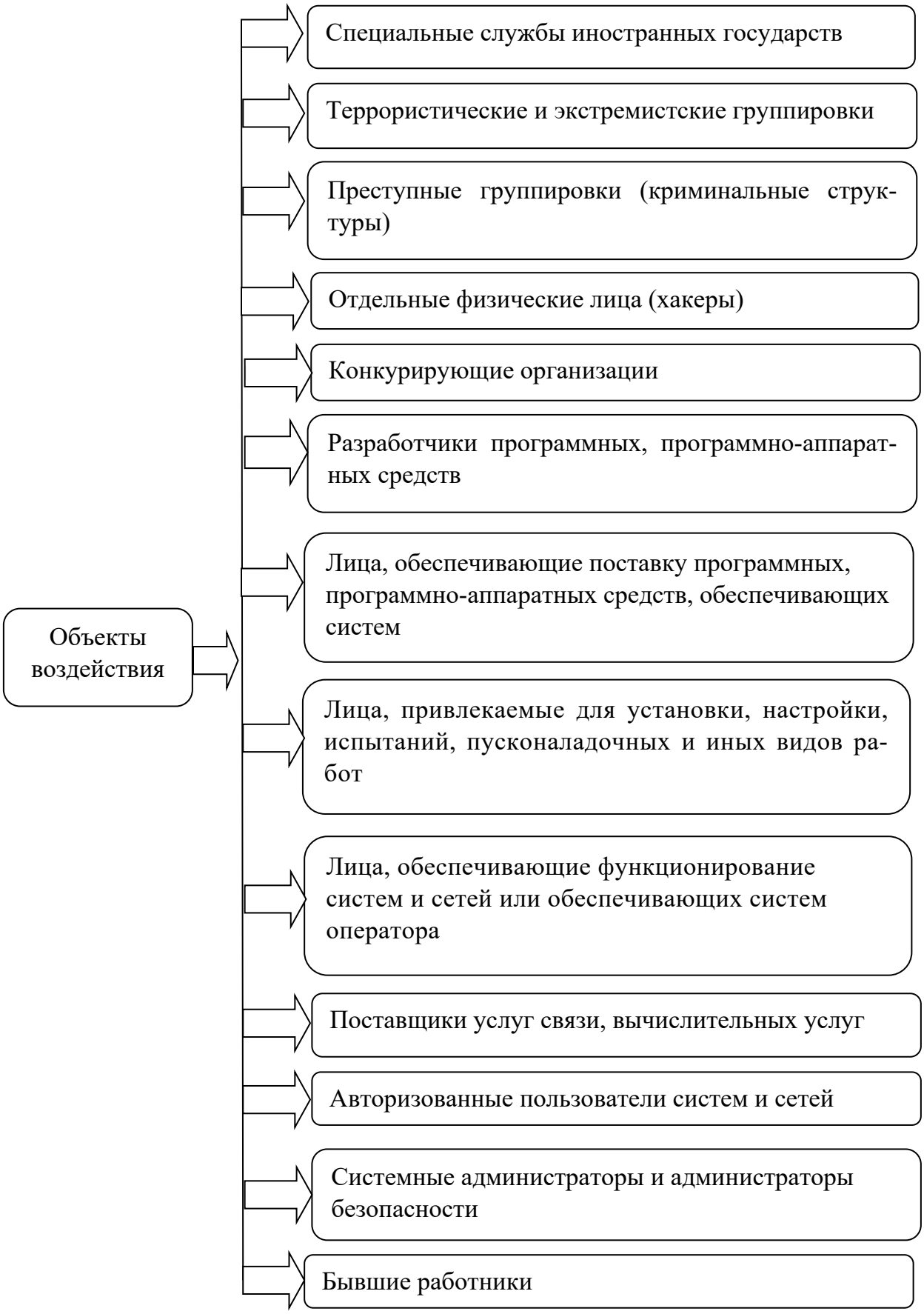


Рис. 9.4. Потенциальные нарушители безопасности информации [17]

Рис. 9.5. Способы реализации угроз безопасности информации [14]

На этапе 3.3 осуществляется определение актуальных угроз безопасности информации экспертным методом. Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для

ПДн. Угрозу можно считать актуальной при выполнении следующих условий [17]:

– наличие нарушителя или иного источника угрозы;

– наличие объекта воздействия (этап 2);

– наличие способа реализации угрозы безопасности информации (этап 3.2);

– наличие негативных последствий при реализации угрозы.

Угроза является возможной, если для нее определены нарушитель, объект воздействия, способ реализации и негативные последствия. Для определения актуальности угроз осуществляется построение сценариев их реализации путем выявления тактик и техник [17].

Порядок выполнения работы

1. Сформируйте экспертную группу из числа студентов вашей группы, количество экспертов должно составлять 4–5 человек. Все описанные ниже этапы проведите экспертным методом.

2. На основе анализа исходных данных экспертным методом определите угрозы безопасности персональных данных [18], а для каждой угрозы установите все виды рисков (ущерба) и возможные негативные последствия от реализации угроз безопасности информации (табл. 9.2) [17]. Данные, приведенные в табл. 9.2, должны быть результатом работы экспертной комиссии.

Таблица 9.2

Список угроз безопасности информации

Номер угрозы	Описание угрозы	Виды рисков (ущерба)	Негативные последствия

3. Для каждой из угроз, перечень которых представлен в табл. 9.2, определите источники угроз безопасности информации (УБИ) категорию и потенциал нарушителей. Итоговые результаты экспертной оценки внесите в табл. 9.3.

Таблица 9.3

Результаты определения источников угроз безопасности информации

Номер УБИ	Вид актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя

4. Оцените цели реализации угроз безопасности информации со стороны нарушителей и их возможные негативные последствия, заполнив табл. 9.4.

Таблица 9.4

Результаты установления возможных негативных последствий

Виды нарушителей	Возможные цели реализации угроз			Соответствие целей видам риска и негативным последствиям
	Физическое лицо	Юридическое лицо, индивидуальный предприниматель	Государство	

5. На основе анализа исходных данных определите объекты и виды воздействия. Для каждой угрозы безопасности информации установите перечень возможных способов реализации (возникновения) угроз безопасности информации (табл. 9.5).

Таблица 9.5

Результаты определения актуальных способов реализации угроз безопасности информации

Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации

6. Определите актуальность установленных угроз безопасности ПДн, заполните табл. 9.6.

Таблица 9.6

Перечень тактик и способов воздействия

Тактика (тактическая задача)	Основные техники (способы) (технические действия)

Отчет должен быть выполнен в электронном варианте и содержать следующие элементы:

1) номер и название практической работы;

2) цель выполнения практической работы;

3) задание, необходимое для выполнения;

4) заполненные табл. 9.3–9.7;

5) вывод о проделанной практической работе.

Контрольные вопросы

1. Приведите характеристику организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Что называют актуальными угрозами? Опишите основные этапы определения актуальных угроз безопасности информации.

3. Приведите основные правила формирования экспертной группы для реализации процедуры определения актуальных угроз безопасности информации.

Практическая работа № 10
ОПРЕДЕЛЕНИЕ ИСХОДНОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДН

Цель работы: определить исходный уровень защищенности информационной системы персональных данных.

Оборудование: учебный персональный компьютер.

Время выполнения: 2 часа.

Общие теоретические сведения

Для оценки возможности реализации угрозы применяются два показателя:

– уровень исходной защищенности ИСПДн (*Y*1);

– частота (вероятность) реализации рассматриваемой угрозы (*Y*2).

Представленная методика была описана в документе [19], однако в настоящее время она отменена. Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Для всех технических и эксплуатационных характеристик ИСПДн экспертным методом устанавливается уровень защищенности (высокий, средний или низкий). Затем для каждого уровня защищенности суммируются положительные решения, рассчитывается доля положительных решений от общего количества решений рассматриваемого уровня защищенности (табл. 10.1).

При установлении исходного уровня защищенности ИСПДн необходимо учитывать следующие условия:

1) в том случае, если для высокого уровня защищенности доля положительных решений составляет 70 % и выше, можно сделать вывод, что ИСПДн имеет высокий уровень защищенности. В этом случае *Y*1 принимает значение, равное 0;

2) в том случае, если 70 % и более положительных решений характерно для уровня «высокий», то можно сделать вывод, что ИСПДн имеет высокий уровень защищенности. Если 70 % и более положительных решений

приходится на уровень «средний», то ИСПДн имеет средний уровень защищенности. В этом случае *Y*1 принимает значение, равное 5;

3) при невыполнении условий, изложенных в п. 1 и 2, ИСПДн имеет низкую степень исходной защищенности. В этом случае *Y*1 принимает значение, равное 10.

Таблица 10.1

Показатели исходного уровня защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
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			

Продолжение табл. 10.1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
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			
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)			

Окончание табл. 10.1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
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			
Количество положительных решений			
Доля положительных решений, %			

Для оценки частоты (вероятности) реализации угроз безопасности информации каждой из них экспертным методом ставится в соответствие числовой коэффициент $Y2$, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Значение коэффициента реализуемости каждой угрозы Y устанавливается соотношением

$$Y = \frac{Y_1 + Y_2}{20}. \qquad (10.1)$$

По результатам оценки коэффициента реализуемости каждой угрозы Y делается вывод о реализуемости рассматриваемых угроз (возможность):

– при $0 \le Y \le 0,3$ – низкая;

– при $0,3 \le Y \le 0,6$ – средняя;

– при $0,6 \le Y \le 0,8$ – высокая;

– при $Y > 0,8$ – очень высокая.

Экспертным методом осуществляется оценка опасности каждой угрозы, которая может быть низкой, средней и высокой в зависимости от

значимости ущерба, наносимого субъекту обработки ПДн при реализации угрозы.

На основании результатов оценки возможности реализации угрозы (*Y*) и опасности угрозы согласно данным методики [13] определяют актуальность каждой угрозы (табл. 10.2).

Порядок выполнения работы

1. Для каждой актуальной угрозы безопасности информации, перечень которых установлен по результатам выполнения практической работы № 4, путем анализа исходных данных оцените уровень исходной защищенности рассматриваемой ИСПДн (*Y*1), заполнив таблицу 10.1.

2. Экспертным методом оцените частоту (вероятность) реализации рассматриваемых актуальных угроз (*Y*2), перечень которых получен вами при выполнении практической работы № 2. Полученные результаты внести в табл. 10.2.

3. На основании установленных значений *Y*1 и *Y*2 рассчитайте значение *Y* для каждой актуальной угрозы безопасности персональных данных. Полученные результаты внесите в табл. 10.2.

Таблица 10.2

Результаты определения уровня защищенности ИСПДн

Обозначение угрозы	*Y*1	*Y*2	*Y*

4. На основании полученных результатов определить актуальность рассмотренных угроз.

Отчет должен быть составлен в электронном варианте и содержать следующие элементы:

1) номер и название практической работы;

2) цель выполнения практической работы;

3) задание для выполнения практической работы;

4) заполненные таблицы 10.1 и 10.2;

5) вывод о проделанной работе.

Контрольные вопросы

1. Что называют исходным уровнем защищенности ИСПДн? Какие нормативно-правовые акты регламентируют процесс установления исходного уровня защищенности ИСПДн?

2. Опишите подробный алгоритм установления исходного уровня защищенности ИСПДн.

3. Для чего применяются результаты установления исходного уровня защищенности ИСПДн?

ЗАКЛЮЧЕНИЕ

В практикуме, предназначенном для изучения дисциплины «Организационные и правовые основы информационной безопасности», приведены практические работы по основным категориям информации ограниченного доступа, в том числе государственной тайне, коммерческой тайне, персональной тайне. В каждой практической работе указана цель ее выполнения, теоретическая и практическая части, вопросы для подготовки к защите практической работы. Работы предполагают подробное изучение законодательной и нормативно-правовой базы по функционированию режима защиты информации ограниченного доступа, определение актуальных угроз безопасности информации. В каждой практической работе приведены формы представления результатов.

Выполнение практических работ направлено на изучение обучающимися законодательных и нормативно-правовых актов, регламентирующих процесс защиты государственной тайны, конфиденциальной тайны и персональных данных в организации; усвоение алгоритма и содержания процедур, принятых в организации для поддержания режима защиты информации ограниченного доступа. Практические работы, представленные в практикуме, основаны на действующей в РФ законодательной базе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Перечень сведений конфиденциального характера: [утв. Указом Президента Российской Федерации от 06.03.1997 № 188]. – М. : Проспект ; СПб. : Кодекс, 1997. – 2 с.

2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: федер. закон № 149-ФЗ : [принят Государственной Думой 08.07.2006 : одобрен Советом Федерации 14.07.2006]. – М. : Проспект ; СПб. : Кодекс, 2006. – 61 с.

3. Российская Федерация. Законы. О государственной тайне : федер. закон № 5485-I : [принят Постановлением Верховного Совета Российской Федерации 21.07.1993]. – М. : Кодекс, 1993. – 45 с.

4. Российская Федерация. Перечень сведений, отнесенных к государственной тайне : [утв. Указом Президента Российской Федерации от 11.02.2006 № 90]. – М. : Кодекс, 2020. – 58 с.

5. Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: официальное издание : утв. Постановлением Правительства Российской Федерации от 04.09.1995 № 870. – М. : Проспект, 1995. – 58 с.

6. О безопасности [Электронный ресурс] : федер. закон от 28.12.2019 № 390-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».

7. Российская Федерация. Конституция Российской Федерации : [принята на всенародном голосовании 12.12.1993) (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)]. – М. : Проспект ; СПб. : Кодекс, 2020. – 94 с.

8. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных : [принята 28.01.1981]. – 14 с.

9. Российская Федерация. Законы. О персональных данных : федер. закон № 152-ФЗ : [принят Государственной Думой 08.07.2006: одобрен Советом Федерации 14.07.2006]. – М. : Проспект ; СПб. : Кодекс, 2006. – 39 с.

10. Российская Федерация. Законы. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке

персональных данных : федер. закон № 160-ФЗ : [принят Государственной Думой 25.11.2005 : одобрен Советом Федерации 07.12.2005]. – М. : Проспект ; СПб. : Кодекс, 2005. – 2 с.

11. Российская Федерация. Трудовой Кодекс Российской Федерации : [принят Государственной Думой 21.12.2001, одобрен Советом Федерации 26.12.2001]. – М. : Проспект ; СПб. : Кодекс, 2001. – 298 с.

12. Специальные требования и рекомендация по технической защите конфиденциальной информации: (СТР-К) : офиц. изд. : утв. решением Коллегии Гостехкомиссии России от 02.02.2001. – М. : Проспект, 2001. – 26 с.

13. Об утверждении требований к защите персональных данных, обрабатываемых в информационных системах персональных данных : офиц. изд. : утв. Постановлением Правительства Российской Федерации от 01.11.2012 № 1119. – М. : Проспект, 2012. – 7 с.

14. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : офиц. изд. : утв. приказом ФСТЭК России от 18.02.2013 № 21. – М. : Проспект, 2013. – 11 с.

15. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : офиц. изд. : утв. приказом ФСТЭК России от 11.02.2013 № 17. – М. : Проспект, 2013. – 37 с.

16. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: (РД) : офиц. изд. : утв. заместителем директора ФСТЭК России от 15.02.2008. – М. : Проспект, 2008. – 73 с.

17. Методический документ. Методика оценки угроз безопасности информации: (МУ) : офиц. изд. : утв. ФСТЭК России от 05.02.2021. – М. : Проспект, 2021. – 85 с.

18. Банк данных угроз безопасности информации [Электронный ъресурс]. – Режим доступа: https://bdu.fstec.ru/threat.

19. Методика определения актуальных угроз безопасности персональных данных при обработке в информационной системе персональных данных: (РД) : офиц. изд. : утв. ФСТЭК России от 14.02.2008.

Приложение 1

СПИСОК ОРГАНИЗАЦИЙ

Номер варианта	Наименование организации
1	ФГБОУ ВО «Сибирский государственный университет геосистем и технологий»
2	ГБУЗ НСО «Центральная клиническая больница»
3	Новосибирский светотехнический завод («Галлоп»)
4	Новосибирский механический завод («Искра»)
5	Кирпичный завод «ЛИКолор»
6	Новосибирский патронный завод
7	Горводоканал
8	Новосибирский стрелочный завод (НСЗ)
9	Новосибирский аффинажный завод (НАЗ)
10	Новосибирский электровозоремонтный завод (Новосибирский ЭРЗ)
11	Новосибирский завод химконцентратов (НЗХК)
12	«Тяжстанкогидропресс» (ТСГП)
13	Коченевская птицефабрика (КПФ)
14	Новосибирский приборостроительный завод
15	Новосибирский металлургический завод им. Кузьмина (НМЗ)
16	Новосибирский инструментальный завод (НИЗ)
17	НПО «Элсиб»
18	«Сиблитмаш»
19	Завод легковозводимых конструкций (ЛВК)
20	«НовоТЭН»
21	«Атом Безопасность»
22	«Инжиниринговые технологии»
23	«Инфовотч»
24	«Инфотекс»

Окончание таблицы

Номер варианта	Наименование организации
25	«Код безопасности»
26	«Конфидент»
27	«КриптоПро»
28	«Лаборатория Касперского»
29	НПП «Гамма»
30	«Перспективный мониторинг»
31	«Ростелеком-Солар»
32	«Эшелон»
33	«Системы информационной безопасности»
34	«Центр финансовых технологий»
35	«Центр защиты информации»
36	«Цифровые технологии»
37	«СмартЛайн»
38	«Серчинформ»
39	«Секью»
40	НТЦ «Атлас»

Приложение 2

Перечень отраслей

Номер варианта	Наименование отрасли
1	Военная
2	Ядерная промышленность
3	Область здравоохранения
4	Образовательная
5	Транспортная
6	Сельскохозяйственная
7	Промышленный и оборонно-промышленный комплекс
8	Энергосбережение
9	Техническое регулирование и обеспечение единства измерений
10	Наука и техника в интересах обороны и безопасности государства
11	Внешняя и внутренняя торговля
12	Внешнеполитическая деятельность
13	Разведывательная, контрразведывательная деятельность
14	Топливно-энергетическая промышленность
15	Черная и цветная металлургия
16	Химическая промышленность
17	Легкая промышленность
18	Пищевая промышленность
19	Добывающая промышленность
20	Обрабатывающая промышленность

Приложение 3

Исходные данные для определения уровня защищенности ИСПДн

Номер варианта	Категория ПДн	Структура ИСПДн	Категория субъектов	Число субъектов ПДн
1	ПДн-Б	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	> 100 000
2	ПДн-Б	Корпоративная распределенная, охватывающая многие подразделения одной организации	Не сотрудников	< 100 000
3	ПДн-Б	Локальная, развернутая в пределах одного здания	Сотрудников	> 100 000
4	ПДн-Б	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	< 100 000
5	ПДн-Б	Локальная, развернутая в пределах одного здания	Сотрудников	< 100 000
6	ПДн-Б	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	> 100 000
7	ПДн-Б	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Сотрудников	< 100 000
8	ПДн-Б	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	> 100 000
9	ПДн-И	Локальная, развернутая в пределах одного здания	Не сотрудников	< 100 000
10	ПДн-И	Городская, охватывающая не более одного населенного пункта (города, поселка)	Сотрудников	> 100 000

Окончание таблицы

Номер варианта	Категория ПДн	Структура ИСПДн	Категория субъектов	Число субъектов ПДн
11	ПДн-И	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	< 100 000
12	ПДн-И	Локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	< 100 000
13	ПДн-И	Локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Не сотрудников	> 100 000
14	ПДн-И	Локальная, развернутая в пределах одного здания	Сотрудников	< 100 000
15	ПДн-И	Локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	> 100 000
16	ПДн-И	Локальная, развернутая в пределах одного здания	Не сотрудников	> 100 000
17	ПДн-О	Локальная (кампусная), развернутая в пределах нескольких близко расположенных зданий	Сотрудников	> 100 000
18	ПДн-О	Корпоративная распределенная, охватывающая многие подразделения одной организации	Сотрудников	> 100 000
19	ПДн-О	Корпоративная распределенная, охватывающая многие подразделения одной организации	Не сотрудников	> 100 000
20	ПДн-О	Распределенная, которая охватывает несколько областей, краев, округов или государство в целом	Не сотрудников	< 100 000

Учебное издание

Троеглазова Анна Владимировна

ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор *О. В. Георгиевская*

Компьютерная верстка *Ю. С. Мерзликиной*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 06.10.2023. Формат 60 × 84 1/16.
Усл. печ. л. 3,48. Тираж 115 экз. Заказ 134.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.