РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный социальный университет» (РГСУ)

ПРИКАЗ

Прохорова Лариса Викторовна

Подписано цифровой подписью: Прохорова Лариса Викторовна
Дата: 2023.07.24 14:34:10 +03'00'

«16» марта 2020 г. № 355

Об утверждении документов, регламентирующих обработку персональных данных в Российском государственном социальном университете

В целях исполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в Российском государственном социальном университете (далее – «РГСУ»)

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Положение об обработке персональных данных в РГСУ (Приложение № 1).

1.2. Модели угроз и нарушителя безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение № 2).

1.3. Акты определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных РГСУ (Приложение № 3).

1.4. Положение о порядке организации и проведении работ по защите персональных данных в РГСУ (Приложение № 4).

1.5. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных (Приложение № 5).

1.6. Перечень персональных данных, обрабатываемых в РГСУ (Приложение № 6).

2. Приказ РГСУ от 26 июля 2013 г. № 751 «Об утверждении Положения об обработке и защите персональных данных в Российском государственном социальном университете» признать утратившим силу.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор **Н.Б. Починок**

Исп. Гасьянч М.А.
Файл: 08 31-3м

Приложение № 1 к приказу
от «16» декабря 2020 г.
№ 355

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «РГСУ»)

ПОЛОЖЕНИЕ
об обработке персональных данных

Москва, 2020 г.

Общие положения

1.1. Назначение документа

Настоящее Положение об обработке персональных данных (далее – Положение) разработано в соответствии со статьей 18.1 Федерального закона от 27 июля 2006 г. № 152 «О персональных данных» и со статьей 86, Трудового Кодекса РФ, определяет порядок обработки персональных данных ФГБОУ ВО РГСУ (далее – Университет), устанавливает требования к защите персональных данных, определяет права, обязанности и ответственность руководителей структурных подразделений и работников.

1.2. Нормативные ссылки

В документе используются положения следующих нормативных актов:

- Трудовой Кодекс Российской Федерации.
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
- Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».
- Федеральный закон 29 декабря 2012 г. от № 273-ФЗ «Об образовании в Российской Федерации».
- Федеральный закон от 03 ноября 2006 г. № 174-ФЗ «Об автономных учреждениях».
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Приказ ФСБ от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).
- «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный приказом Министерства культуры Российской Федерации № 558 от 25 августа 2010 г.

1.3. Область действия

Действие настоящего Положения распространяется на персональные данные, обрабатываемые Университетом как с использованием средств автоматизации, так и без использования таких средств.

Все работники Университета, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись в

Журнале учета ознакомления должностных лиц с правилами обеспечения безопасности персональных данных (Приложение № 1 к настоящему Положению).

1.4. Термины, определения и сокращения

• **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

• **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.

• **Персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

• **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, подлежащих обработке, действия (операции), совершаемые с персональными данными.

• **Субъект персональных данных** – физическое лицо, в отношении которого в соответствии с законом осуществляется обработка его персональных данных.

1.5. Утверждение и пересмотр

Настоящее Положение вступает в силу с момента его утверждения приказом Университета и действует бессрочно до замены его новым Положением.

Пересмотр Положения производится в следующих случаях:

• при изменении процессов и технологий обработки персональных данных в Университете;

• по результатам проверок органа по защите прав субъектов персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности персональных данных;

• при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности персональных данных;

• в случае выявления существенных нарушений по результатам внутренних проверок системы защиты персональных данных.

Ответственным за пересмотр данного Положения является работник Университета, назначенный ответственным за организацию обработки персональных данных в Университете. Измененное Положение утверждается приказом Ректора ФГБОУ РГСУ, либо лицом, его заменяющим.

2. Обработка персональных данных

2.1. Общий порядок обработки

Приказом Университета, назначается лицо, ответственное за организацию обработки персональных данных.

Обработка персональных данных в структурных подразделениях ФГБОУ РГСУ ведётся в объёме, определяемом функционалом подразделений. Работники Университета допускаются к обработке персональных данных в объёме, определяемом должностными обязанностями.

При определении объема и содержания обрабатываемых персональных данных Университет руководствуется Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных», Федеральным законом от 27 июля 2010 г. № 210 «Об организации предоставления государственных и муниципальных услуг» и другими нормативными актами. Объем и содержание, обрабатываемых персональных данных, способы обработки персональных данных, должны соответствовать целям обработки персональных данных.

В ФГБОУ РГСУ ведётся обработка персональных данных в информационных системах персональных данных (ИСПДн):

- ИСПДн «Кадры».
- ИСПДн «Обучающиеся».
- ИСПДн «Абитуриенты».
- ИСПДн «Контрагенты».
- ИСПДн «Медицина».
- ИСПДн «СКУД».
- ИСПДн «Отдых и проживание».
- ИСПДн «Абилимпикс».

2.2. Получение (сбор) персональных данных

В Университете производится обработка персональных данных следующих категорий субъектов персональных данных:

- работники РГСУ;
- соискатели вакансий;
- уволенные работники РГСУ;
- члены семей работников РГСУ;
- контрагенты РГСУ;
- работники контрагентов РГСУ;
- студенты РГСУ;
- абитуриенты РГСУ;
- пациенты поликлиники РГСУ;
- иные получатели услуг РГСУ.

Для каждой категории субъектов персональных данных определены цели обработки и содержание обрабатываемых персональных данных.

Целями обработки персональных данных работников Университета являются:

- ведение кадрового делопроизводства;
- начисление и выплата заработной платы, стипендии, вознаграждений, премирования, материальной помощи;
- начисление взносов в пенсионный фонд, фонд социального страхования;
- начисление налога на доход физических лиц;
- формирование отчетности для предоставления в государственные органы;
- обеспечение общехозяйственной деятельности;
- обеспечение экономической, физической, пожарной, информационной безопасности;
- предотвращение конфликта интересов.

Университет осуществляет сбор следующих персональных данных своих работников:

- фамилия, имя, отчество;
- тип, серия, номер документа, удостоверяющего личность;
- дата выдачи документа, удостоверяющего личность;
- год, месяц, дата, место рождения;
- адрес регистрации по месту жительства и/или по месту пребывания;
- контактная информация, в том числе номер контактного телефона и адрес электронной почты;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства государственного пенсионного страхования;
- доходы
- должность;
- фотография;
- образование;
- профессия;
- табельный номер;
- банковские реквизиты

• номер профсоюзного билета;

• статус воинского учета, отношение к воинской обязанности, категория годности к военной службе, районный военный комиссариат, категория запаса состав (профиль), полное кодовое обозначение военной учетной специальности, сведения о воинском учете;

• семейное положение;

• трудовой стаж;

• сведения о пребывании за границей;

• данные о социальных льготах;

• данные полиса ОМС;

• сведения об оказанных услугах;

• гражданство;

• данные разрешения на временное проживание;

• тарифная ставка/оклад;

• сведения об аттестации и повышении квалификации;

• сведения об отчислениях в ФНС, ПФР и ФСС.

Целями обработки персональных данных уволенных работников Университета являются:

• ведение кадрового делопроизводства;

• формирование отчетности для предоставления в государственные органы.

Целями обработки персональных данных членов семей работников Университета являются:

• учет налоговых льгот при начислении заработной платы;

• исполнение обязанностей работодателя при возникновении несчастного случая.

Университет осуществляет сбор следующих персональных данных членов семей работников Университета:

• фамилия, имя, отчество;

• степень родства;

• год, месяц, дата рождения.

Целью обработки персональных данных соискателей вакансий Университета является заключение трудового договора.

ФГБОУ РГСУ осуществляет сбор следующих персональных данных соискателей вакансий Университета:

• фамилия, имя, отчество;

• дата и место рождения;

• паспортные данные;

• адрес регистрации по месту жительства;

• фактический адрес;

• контактные данные;

• семейное положение;

• состав семьи;

• сведения об образовании;

• трудовой опыт

Целью обработки персональных данных контрагентов и работников контрагентов Университета является оформление и исполнение договорных обязательств.

Университет осуществляет сбор следующих персональных данных контрагентов и работников контрагентов:

• фамилия, имя, отчество;

• должность;

• контактная информация;

• сведения о месте жительства,

• паспортные данные;

• ИНН;

- реквизиты лицевого счета в банке;
- сведения о доходах.

Целью обработки персональных студентов (обучающихся) и абитуриентов является предоставление образовательных услуг в соответствии с требованиями Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» и Федерального закона от 03 ноября 2006 г. № 174-ФЗ «Об автономных учреждениях».

Университет осуществляет сбор следующих персональных данных обучающихся:

- фамилия, имя, отчество;
- тип, серия, номер документа, удостоверяющего личность;
- дата выдачи документа, удостоверяющего личность, информация о выдавшем его органе;
- год, месяц, дата и место рождения;
- адрес регистрации по месту жительства и/или по месту пребывания
- номер контактного телефона;
- адрес электронной почты;
- фотография;
- образование;
- профессия;
- табельный номер;
- идентификационный номер налогоплательщика;
- банковские реквизиты;
- номер профсоюзного билета;
- статус воинского учета;
- отношение к воинской обязанности;
- категория годности к воинской службы;
- районный военный комиссариат;
- категория запаса;
- воинское звание, состав (профиль);
- полное кодовое обозначение военной учетной специальности;
- номер страхового свидетельства государственного пенсионного страхования;
- состояние здоровья;
- социальное положение;
- данные полиса ОМС;
- сведения об оказанных услугах;
- семейное положение.

В том числе несовершеннолетних:

- фамилия, имя, отчество;
- тип, серия, номер документа, удостоверяющего личность;
- дата выдачи документа, удостоверяющего личность, информация о выдавшем его органе;
- год, месяц, дата и место рождения;
- адрес регистрации по месту жительства и/или по месту пребывания;
- номер контактного телефона;
- адрес электронной почты;
- фотография;
- образование;
- профессия;
- табельный номер;
- идентификационный номер налогоплательщика;
- состояние здоровья;
- социальное положение;
- данные полиса ОМС;

- сведения об оказанных услугах;
- приписное свидетельство;
- семейное положение.

Университет осуществляет сбор следующих персональных данных абитуриентов:

- фамилия, имя, отчество;
- факультет/институт/филиал (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- анкетные и биографические данные;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность (аспирантов, обучающихся);
- занимаемая должность (аспирантов, обучающихся);
- адрес по месту фактического проживания;
- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;
- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение (содержащееся в личном деле, студенческом билете, пропуске, зачетной книжке обучающегося);
- банковские реквизиты обучающегося;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- сведения по отпускам (академический);
- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья;
- иные сведения, с которыми абитуриент и обучающийся считает нужным ознакомить ФГБОУ ВО РГСУ, либо дополнительная информация необходимая Университету.

Целью обработки персональных данных пациентов Поликлиники РГСУ является предоставление медицинских услуг, в соответствии с которым предоставление медицинской услуги осуществляется после однократного обращения заявителя с соответствующим запросом, а взаимодействие с органами, предоставляющими государственные услуги, осуществляется Университетом без участия заявителя в соответствии с нормативными правовыми актами и соглашением о взаимодействии.

Университет осуществляет сбор следующих персональных данных пациентов РГСУ:

- фамилия имя отчество;
- сведения о документе, удостоверяющем личность;
- контактная информация;
- дата и место рождения;

- паспортные данные;
- пол;
- место жительства;
- данные миграционной карты;
- инвалидность;
- семейное положение;
- диагноз санатория;
- жалобы больного;
- история настоящего заболевания;
- стационарное лечение;
- санаторно-курортное лечение;
- перенесенные заболевания;
- наследственность;
- объективные данные (рост, масса тела, телосложение, кожные покровы и т.д.);
- состояние здоровья;
- предварительный диагноз;
- назначение врача;
- итоги лечения;
- сведения о регистрации;
- данные разрешения на временное проживание;
- ИНН;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения о детях и родственниках;
- иные сведения, предусмотренные трудовым законодательством и законодательством об организации предоставления медицинских услуг.

Целью обработки персональных данных иных получателей услуг является предоставление услуг по проживанию или временному размещению.

Университет осуществляет сбор следующих персональных данных пользователей гостиничных и иных услуг ФГБОУ ВО РГСУ:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- номер контактного телефона;
- адрес электронной почты;
- данные о месте работы (при бронировании командируемых юридических лиц и ИП);
- номер банковской карты (в случае оплаты услуг отеля таковой).

Персональные данные могут быть получены:

- лично у субъекта персональных данных;
- у законного представителя субъекта персональных данных;
- в органе, предоставляющем государственные услуги, органе, предоставляющем муниципальные услуги, ином государственном органе, органе местного самоуправления, подведомственных государственным органам или органам местного самоуправления организациях, участвующих в предоставлении государственных и муниципальных услуг.

Если предоставление персональных данных является обязательным в соответствии с Федеральным законом, Университет обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные. Типовая форма разъяснения представлена в Приложении № 2 к настоящему Положению.

В случае получения персональных данных от представителя субъекта персональных данных полномочия данного представителя проверяются оператором.

Если для осуществления своей деятельности необходимо получить документы или информацию об ином лице, не являющемся заявителем, заявитель должен представить

письменное согласие такого лица или его законного представителя на обработку его персональных данных (Приложение № 4 к настоящему Положению).

Запрещается требовать от лиц, поступающих на работу, документы, помимо предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

Не допускается обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных ч. 2 ст. 10. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», среди которых в том числе:

• субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

• персональные данные сделаны общедоступными субъектом персональных данных;

• обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

• обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

• обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

При принятии решений, затрагивающих интересы субъекта персональных данных, Университет не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки, за исключением следующих случаев: решение принято на основании исключительно автоматизированной обработки персональных данных при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Оператор обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

2.3. Доступ к персональным данным

Работники, доступ которых к персональным данным, обрабатываемым в информационной системе Университета необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании перечня, утвержденного Ректором ФГБОУ ВО РГСУ, либо лицом, его заменяющим, и только после подписания обязательства о неразглашении персональных данных (Приложение № 12 к настоящему Положению).

Работники, имеющие доступ к персональным данным, имеют право получать и обрабатывать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций.

В случае, если Университет пользуется услугами юридических и физических лиц на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным, обрабатываемым в Университете, то соответствующие данные предоставляются Университетом только после подписания с ними

соглашения о неразглашении конфиденциальной информации или включения в договоры пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных.

Государственным органам, осуществляющим функции контроля (надзора) предоставляют права доступа к персональным данным, обрабатываемым в Университете только в сфере их компетенции и в объеме, предусмотренном действующим законодательством.

Субъект персональных данных, сведения о котором обрабатываются в Университете, имеет право на получение информации касающейся обработки его персональных данных. Субъект персональных данных вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. Обращение субъекта фиксируется в журнале учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационной системе персональных данных ФГБОУ ВО РГСУ. Уведомление субъекта персональных данных о блокировке, о невозможности прекращения обработки и уничтожения, о прекращении обработки и уничтожении, о внесении изменений в его персональные данные осуществляется по формам согласно Приложениям № 8-11 к настоящему Положению.

Сведения, предоставляемые субъекту, должны быть в доступной форме, и не должны содержать персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, при которых имеются законные основания для раскрытия таких персональных данных.

Университет обязан в порядке, предусмотренном Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных», сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

2.4. Передача персональных данных

Запрещается передавать персональные данные третьим лицам без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, установленных законодательством РФ.

Документы, содержащие персональные данные субъекта, могут быть отправлены в сторонние организации курьером (работником Университета) или через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Так, в случае отправления документов посредством федеральной почтовой связи, они вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

Внутри Университета без письменного согласия субъекта персональных данных разрешается передача (предоставление) персональных данных в структурные подразделения, необходимые им для выполнения своих функций.

Лица, получающие персональные данные, должны быть предупреждены, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности (данное требование не распространяется на обмен персональными данными субъектов персональных данных в порядке, установленном федеральным законодательством).

Разрешается передавать персональные данные представителям субъектов персональных данных в порядке, установленном существующим законодательством, и ограничивать эту информацию данными, необходимыми для выполнения указанными представителями их функций.

Трансграничная передача персональных данных (при возникновении необходимости) осуществляется в соответствии с требованиями действующего законодательства (ст. 12 Федерального закона от 27 июня 2006 г. № 152-ФЗ «О персональных данных»).

Трансграничная передача персональных данных на территории иностранных государств осуществляется в случае наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных.

2.5. Порядок обработки персональных данных без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Работники Университета, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также настоящим Положением.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес организации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Университетом способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, предпринимаются меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных

данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

• при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Данные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

2.6. Сроки хранения персональных данных

Сроки хранения персональных данных ФГБОУ ВО РГСУ установлены в рамках процессов архивного хранения документов (приказом Министерства культуры РФ от 25.08.2010 №558 «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»).

Действие Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использование содержащих персональные данные архивных документов, в соответствии с законодательством об архивном деле в РФ. Таким образом сроки хранения информации, являющейся персональными данными, определяются структурными подразделениями. Если заявитель в течение года не прибыл для получения результата услуги, результат услуги отправляется обратно в структурное подразделение на ответственное хранение в составе дела, откуда выдается при обращении заявителя за его получением.

Книги учета выдачи результатов услуг хранятся постоянно.

Документы на бумажных носителях, содержащие персональные данные работников и/или контрагентов, хранятся в течение времени, установленного трудовым законодательством и законодательством о бухгалтерском учете. В информационной системе персональные данные работников хранятся в течение трех лет со дня увольнения работника.

Персональные данные соискателя вакансии Университета в виде бумажных либо электронных анкет хранятся до тех пор, пока существует потенциальная возможность заключения трудового договора с данным лицом.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем требуется для достижения цели обработки персональных данных.

2.7. Порядок уничтожения персональных данных

Уничтожение документов, содержащих персональные данные, производится:

• по достижении целей их обработки;

• по достижении окончания срока хранения персональных данных, оговоренного в соответствующем соглашении заинтересованных сторон;

• в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

Уничтожение персональных данных, находящихся на машинных носителях информации, выполняется средствами информационной системы (операционной системы, системы управления базами данных).

Уничтожение машинных носителей с персональными данными осуществляется согласно Положению об использовании материальных носителей персональных данных Университета.

Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов. Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2-х человек. Уничтожение осуществляется по акту. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

2.8. Особенности обработки персональных данных работников Университета

В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу, ее прохождением, увольнением и необходимые для обеспечения деятельности ФГБОУ ВО РГСУ.

Личные дела действующих и уволенных работников Университета хранятся раздельно в сейфах или шкафах, обеспечивающих защиту от несанкционированного доступа.

К личному делу приобщают:

• фотографию;

• анкету;

• копию паспорта;

• копию военного билета;

• копию СНИЛС;

• копию ИНН;

• копии документов об образовании;

• копии свидетельств о рождении детей;

• копию свидетельства о регистрации по месту пребывания;

• копии свидетельств о государственной регистрации актов гражданского состояния;

• заявления о приеме/переводе/увольнении;

• приказы о назначении/переводе/увольнении;

• экземпляр трудового договора;

• экземпляры письменных дополнительных соглашений о внесении изменений и дополнений в трудовой договор;

• служебные записки о перемещении по службе;

• документы о повышении квалификации;

• дополнения к личному листку по учету кадров;

• обязательство о неразглашении ПДн;

• согласие на обработку ПДн;

• карточку Т-2;

• внутреннюю опись документов.

Все документы личного дела подшиваются в папку, на обложке которой указываются фамилия, имя, отчество работника, номер личного дела. Документы, поступающие в личное дело, располагаются в хронологическом порядке, листы нумеруются.

В обязанности работника, осуществляющего ведение личных дел работников, входит:

• приобщение документов к личным делам работников;

• обеспечение сохранности личных дел работников;

• обеспечение конфиденциальности сведений, содержащихся в личных делах работников, в соответствии с законодательством РФ, а также в соответствии с настоящим Положением.

Личное дело ведется на протяжении всей трудовой деятельности работника в Университете. Персональные данные работников могут обрабатываться в электронном виде в информационной системе персональных данных ФГБОУ ВО РГСУ.

Сроки хранения персональных данных работников определяются на основании «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденного приказом Министерства культуры Российской Федерации от 25 августа 2010 г. № 558

3. Обязанности лиц, допущенных к обработке персональных данных

Работники, допущенные к обработке персональных данных, обязаны:

- знать и выполнять требования настоящего Положения;
- осуществлять обработку персональных данных в целях, определенных данным Положением (п. 2.2);
- знакомиться только с теми персональными данными, к которым получен допуск;
- хранить в тайне известные им сведения о субъектах персональных данных, информировать своего непосредственного начальника о фактах нарушения порядка обработки персональных данных и о попытках несанкционированного доступа к ним;
- предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- выполнять требования по защите полученных персональных данных;
- соблюдать правила пользования документами, содержащими персональные данные, порядок их обработки и защиты;
- предоставлять письменные объяснения о допущенных нарушениях установленного порядка обработки персональных данных, а также о фактах их разглашения.

4. Обеспечение безопасности персональных данных

4.1. Принципы обеспечения безопасности персональных данных

Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается ФГБОУ ВО РГСУ в установленном законодательством РФ и локальными нормативными актами Университета порядке, выполнением комплекса организационных и технических мер, обеспечивающих их безопасность.

Меры по обеспечению информационной безопасности персональных данных при их обработке распространяются как на бумажные, так и на машинные носители информации.

Для осуществления мероприятий по обеспечению безопасности персональных данных приказом Университета назначается лицо, ответственное за защиту информации.

Организацию защиты персональных данных в структурных подразделениях обеспечивают руководители подразделений.

Получение и обработка уполномоченными лицами персональных данных производится после подписания субъектом персональных данных согласия (Приложения № 3-7, 15, 16 к настоящему Положению) в случаях, если это требуется законодательством РФ.

4.2. Меры по обеспечению безопасности персональных данных

Хранение персональных данных в Университет осуществляется в порядке, исключающем к ним доступ третьих лиц, их утрату или их неправомерное использование.

Помещения, в которых ведется обработка персональных данных, должны обеспечивать их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц.

В течение рабочего дня ключи от шкафов (ящиков, хранилищ), в которых содержатся носители персональных данных, а также помещений, где находятся средства вычислительной техники, предназначенные для обработки персональных данных, находится на хранении у ответственных работников.

По окончании рабочего времени помещения, предназначенные для обработки персональных данных должны быть закрыты на ключ, бесконтрольный доступ в такие помещения должен быть исключен, в том числе применением опечатывания, видеонаблюдения или систем контроля доступа.

Университетом осуществляется учет машинных носителей персональных данных.

Организация защиты персональных данных, обрабатываемых в информационных системах персональных данных, осуществляется в рамках действующей в ФГБОУ ВО РГСУ системы защиты информации.

Доступ к информационным системам персональных данных защищается системой паролей, а также программно-аппаратными средствами защиты информации.

Использование в сети Университета мобильных устройств и технологий беспроводного доступа (Wi-Fi, Bluetooth, 3G и т.п.) согласовывается с Ответственным за защиту информации, обеспечивается выявление их несанкционированного подключения к сети Университета.

В отношении каждой категории персональных данных приказом ФГБОУ ВО РГСУ, либо лица, его заменяющего, определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, ответственных за доступ к ним.

Университетом обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Для обеспечения таких условий принимаются следующие меры:

- исключается возможность бесконтрольного проникновения посторонних лиц в места хранения материальных носителей;
- в течение рабочего дня ключи от шкафов (ящиков, хранилищ) и помещений, в которых содержатся материальные носители, находятся на хранении у ответственных работников;
- по окончании рабочего времени помещения, предназначенные для хранения материальных носителей, закрываются на ключ.

Ответственным за реализацию указанных мер является Ответственный за организацию обработки персональных данных в Университете.

4.3. Порядок осуществления взаимодействия, сопровождающего предоставление персональных данных

Любое соединение с внешней информационной системой должно быть согласовано с Ответственным за защиту информации. Любой доступ должен быть ограничен и протестирован на возможные уязвимости. Внешний доступ должен также отвечать следующим характеристикам:

- третьи стороны должны подписывать соглашение о взятии на себя обязательств по обеспечению информационной безопасности своей части сети, соединенной с сетью Университета, а также соглашение о неразглашении персональных данных;
- должны быть обеспечены контроль доступа и аутентификация.

Передача персональных данных по незащищенным каналам связи запрещается.

В целях обеспечения информационной безопасности Университета при взаимоотношении с третьими лицами должны обеспечиваться действующие правила и меры по обеспечению информационной безопасности, и выполняться следующие меры:

- должно заключаться соглашение о неразглашении персональных данных;
- по возможности должен проводиться мониторинг действий третьих лиц в информационных системах Университета;
- по возможности предусмотреть в договорах с третьими лицами право Университета на проведение аудита обеспечения информационной безопасности той информации, которую Университет передает третьему лицу;
- обязателен к ведению журнал учета материальных носителей информации, переданных третьим лицам и содержащих персональные данные.

В случае заключения договора с юридическим лицом, предметом которого является передача информации, принадлежащей Университету на законных основаниях, Университет должен удостовериться до заключения договора в адекватном уровне обеспечения информационной безопасности юридическим лицом. Адекватным уровнем может являться: наличие аудиторского заключения независимого аудитора уровня информационной безопасности как юридического лица в целом, так и отдельного направления деятельности в частности.

5. Права субъектов на защиту своих персональных данных

В целях обеспечения защиты своих персональных данных субъект имеет право:

- на получение сведений, касающихся обработки его персональных данных, в соответствии с частью 7 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- получить сведения, предоставляемые Университетом субъекту о его персональных данных, в доступной форме;
- требовать немедленно прекратить по обработку персональных данных субъекта, взятых без предварительного согласия, если иное не установлено Федеральным Законом;
- дать или отказаться дать письменное согласие на исключительно автоматизированную обработку данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
- обжаловать действия или бездействие Университета в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке при осуществлении обработки персональных данных субъекта с нарушением законодательства и/или нарушением его прав и свобод.
- вносить предложения по мерам защиты персональных данных.

6. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Должностные лица, имеющие доступ к персональным данным, несут личную ответственность за нарушение режима защиты персональных данных в соответствии с законодательством Российской Федерации.

Каждый работник Университета, получающий для работы содержащий персональные данные документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Работники Университета, которым сведения о персональных данных стали известны в силу их служебного положения, несут ответственность за их разглашение.

Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера, работодатель вправе применять предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.

Ответственность за соблюдение вышеуказанного порядка обработки персональных данных несет работник, а также руководитель структурного подразделения, осуществляющего обработку персональных данных.

Должностные лица, в обязанность которых входит обработка персональных данных работников Университета, обязаны обеспечить каждому работнику, при необходимости, возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7. Контроль выполнения требований настоящего Положения

Повседневный контроль порядка обращения с персональными данными осуществляют руководители тех структурных подразделений Университета, в которых обрабатываются персональные данные субъектов.

Периодический контроль выполнения настоящего Положения возлагается на должностное лицо, назначенное приказом ФГБОУ ВО РГСУ, ответственным за организацию обработки персональных данных.

Приложение № 1 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Журнал учета ознакомления должностных лиц с правилами обеспечения безопасности персональных данных

№ п/п	Наименование документа/обучения	Дата	Должность и ФИО работника, ознакомившегося с документом/ прошедшего обучение	Подпись
1	2	3	4	5

Приложение № 2 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Форма разъяснений субъекту персональных данных юридических последствий отказа предоставить его персональные данные

Кому: _____

_____

Адрес: _____

_____

РАЗЪЯСНЕНИЯ
юридических последствий отказа предоставить персональные данные

Уважаемый (ая) _____,

уведомляем Вас о том, что оператору персональных данных ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ): 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, требуется получить следующие персональные данные:

_____
(перечень персональных данных)

на основании следующих федеральных законов:

_____,
(перечень документов)

В случае отказа предоставить перечисленные персональные данные:

_____
(перечень юридических последствий)

_____.

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение № 3 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «10» января 2020 г.
№ 355

Согласие субъекта (работника) на обработку его персональных данных

Я, _____, паспорт серии _____, номер _____, выданный _____ «___»_____ _____ года, проживающий(ая) по адресу: _____, в соответствии с Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных» даю согласие ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), зарегистрированному по адресу 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- фотография;
- контактная информация;
- дата и место рождения;
- информация о месте жительства;
- паспортные данные;
- пол;
- гражданство;
- должность;
- данные разрешения на временное проживание;
- номер страхового свидетельства государственного пенсионного страхования;
- ИНН;
- тарифная ставка/оклад;
- семейное положение;
- сведения о детях и родственниках;
- сведения о воинском учете;
- сведения об образовании;
- сведения об аттестации и повышении квалификации;
- сведения о трудовой деятельности;
- сведения об отчислениях в ФНС, ПФР и ФСС;
- реквизиты лицевого счета в банке;
- сведения о доходах;
- сведения о социальных льготах.

Целями обработки персональных данных являются:

- ведение кадрового делопроизводства;
- начисление и выплата заработной платы, вознаграждений, премирования, материальной помощи;
- начисление взносов в пенсионный фонд, фонд социального страхования;
- начисление налога на доход физических лиц;
- формирование отчетности для предоставления в государственные органы;
- обеспечение общехозяйственной деятельности;
- обеспечение экономической, физической, пожарной, информационной безопасности;

- предотвращение конфликта интересов.

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (в том числе предоставление определенному кругу третьих лиц для достижения вышеуказанных целей), обезличивание, блокирование, удаление, уничтожение, осуществляемых как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

Согласен(а) на размещение в общедоступных источниках, следующих моих персональных данных: фамилия, имя, отчество, должность, номер рабочего телефона, фотография.

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с политикой ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания на период не менее, чем срок хранения документов, установленных архивным законодательством.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

«__» _____ 20__ г. _____ (_____)

(подпись, расшифровка подписи)

Приложение № 4 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Согласие субъекта (обучающегося) на обработку его персональных данных

ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ)
129226, г. Москва, ул. Вильгельма Пика, дом 4, стр. 1

Согласие на обработку персональных данных

В соответствии с частью 4 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

я, _____, паспорт серии _____, номер _____, выданный _____ «___»_____ _____ года, проживающий(ая) по адресу: _____,

даю согласие ФГБОУ ВО РГСУ, зарегистрированному по 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество
- паспортные данные;
- дата и место рождения;
- личная фотография;
- гражданство;
- сведения о месте жительства (по месту регистрации, фактическое);
- контактная информация (телефон, электронный адрес);
- семейное и социальное положение;
- сведения о составе и членах семьи (степень родства, ФИО, место работы, должность, адрес, телефон);
- сведения об образовании, о наличии специальных знаний, свидетельство о результатах единого государственного экзамена, данные о результатах вступительных испытаний, данные о процессе обучения и успеваемости;
- сведения о трудовой деятельности, стаже;
- ИНН, СНИЛС;
- сведения о наградах, присвоенных званиях;
- сведения о социальных льготах;
- сведения о воинской обязанности, в том числе сведений, содержащийся в военном билете, приписном свидетельстве и других документах, выдаваемых ведомствами и структурами Министерства Обороны;
- сведения, подтверждающий льготный статус, и сведения о состоянии здоровья;
- сведения о стипендии.

Целью обработки персональных данных является предоставление образовательных услуг в соответствии с требованиями Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» и Федерального закона от 3 ноября 2006 года № 174-ФЗ «Об автономных учреждениях».

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор (в том числе у определенного круга третьих лиц, без уведомления меня об этом), систематизацию, накопление, хранение, уточнение (обновление,

изменение), использование, предоставление (в том числе передачу определенному кругу третьих лиц для достижения вышеуказанных целей), обезличивание, блокирование, удаление, уничтожение. Оператор вправе обрабатывать мои персональные данные как с использованием средств автоматизации, так и без использования таких средств.

Также настоящим согласием я разрешаю включить мои персональные данные в общедоступные источники (справочники) и внутренние информационно-справочные ресурсы ФГБОУ ВО РГСУ в целях информационного обмена на время моего обучения в ФГБОУ ВО РГСУ не более чем в следующем объеме:

- фамилия, имя, отчество;
- дата рождения;
- контактная информация (телефон, адрес электронной почты);
- фотография;
- сведения о наградах, присвоенных званиях;
- сведения о процессе обучения и успеваемости;
- сведения о курсе и специализации обучения.

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие дано мной _____.
(дата)

Согласие действует _____.
(срок действия)

«__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Принял: «__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Приложение № 5 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 353

Согласие субъекта (абитуриента) на обработку его персональных данных

ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ)
129226, г. Москва, ул. Вильгельма Пика, дом 4, стр. 1

Согласие на обработку персональных данных

В соответствии с частью 4 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

я, _____, паспорт серии _____, номер _____, выданный _____ «___»_____ _____ года, проживающий(ая) по адресу: _____,

даю согласие ФГБОУ ВО РГСУ, зарегистрированному по 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- факультет/институт/филиал (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- анкетные и биографические данные;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность (аспирантов, обучающихся);
- занимаемая должность (аспирантов, обучающихся);
- адрес по месту фактического проживания;
- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;
- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение (содержащееся в личном деле, студенческом билете,
- пропуске, зачетной книжке обучающегося);
- банковские реквизиты обучающегося;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- сведения по отпускам (академический);

- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья.

Целью обработки персональных данных является предоставление образовательных услуг в соответствии с требованиями Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» и Федерального закона от 3 ноября 2006 года № 174-ФЗ «Об автономных учреждениях».

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор (в том числе у определенного круга третьих лиц, без уведомления меня об этом), систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (в том числе передачу определенному кругу третьих лиц для достижения вышеуказанных целей), обезличивание, блокирование, удаление, уничтожение. Оператор вправе обрабатывать мои персональные данные как с использованием средств автоматизации, так и без использования таких средств.

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие дано мной _____.
(дата)

Согласие действует _____.
(срок действия)

«__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Принял: «__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Приложение № 6 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 353

Согласие субъекта (представителя субъекта) на обработку его персональных данных в медицинских целях

ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ)
129226, г. Москва, ул. Вильгельма Пика, дом 4, стр. 1

Согласие на обработку персональных данных

В соответствии с частью 3 статьи 13 Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», части 4 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

я, _____, паспорт серии _____, номер _____, выданный _____

«___» _____ _____ года, проживающий(ая) по адресу: _____, даю согласие ФГБОУ ВО РГСУ, зарегистрированному по адресу 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- сведения о документе, удостоверяющем личность;
- контактная информация;
- дата и место рождения;
- паспортные данные;
- пол;
- место жительства;
- данные миграционной карты;
- сведения о регистрации;
- данные разрешения на временное проживание;
- ИНН;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения о детях и родственниках.

В том числе специальные категории персональных данных:

- инвалидность;
- история настоящего заболевания;
- стационарное лечение;
- санаторно-курортное лечение;
- перенесенные заболевания;
- наследственность;
- объективные данные (рост, масса тела, телосложение, кожные покровы и т.д.);
- состояние здоровья;
- предварительный диагноз;
- назначение врача;
- итоги лечения.

Целью обработки персональных данных является предоставление медицинских услуг.

Согласен(а) на предоставление моих персональных данных органам, предоставляющим государственные услуги, органам, предоставляющими муниципальные услуги, иным

государственным органам, органам местного самоуправления, подведомственным государственным органам или органам местного самоуправления организацией, участвующим в предоставлении государственных и муниципальных услуг.

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор (в том числе у определенного круга третьих лиц, без уведомления меня об этом), систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (в том числе передачу определенному кругу третьих лиц для достижения вышеуказанных целей), обезличивание, блокирование, удаление, уничтожение. Оператор вправе обрабатывать мои персональные данные как с использованием средств автоматизации, так и без использования таких средств.

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с политикой ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ согласно части 2 статьи 9 «О персональных данных».

Настоящее согласие дано мной _____.
(дата)

Согласие действует _____.
(срок действия)

«__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Принял: «__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Приложение № 7 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «10» марта 2020 г.
№ 355

Согласие субъекта (соискателя вакансии) на обработку его персональных данных

Я,_____, паспорт серии _____, номер _____, выданный _____ «___»_____ _____ года, проживающий(ая) по адресу: _____, в соответствии с Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных» даю согласие ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), зарегистрированному по адресу129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- адрес по прописке;
- фактический адрес;
- контактные данные;
- семейное положение;
- состав семьи;
- сведения об образовании
- трудовой опыт.

Целью обработки персональных данных является содействие в заключении трудового договора.

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, блокирование, удаление, уничтожение, осуществляемых как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с политикой ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания на период не менее чем срок хранения документов, установленных архивным законодательством.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ согласно части 2 статьи 9 «О персональных данных».

«__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

Приложение № 8 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 353

Форма уведомления субъекта персональных данных о блокировании его персональных данных

В соответствии с ч. 3 ст. 20 и ч. 2 ст. 21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»

Кому: _____

_____

Адрес: _____

_____

УВЕДОМЛЕНИЕ

О блокировании персональных данных

Уважаемый (ая) _____,

уведомляем Вас о том, что оператор персональных данных ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), юридический адрес: 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, произвел блокирование Ваших персональных данных, а именно:

№ п.п.	Исходные данные	Новые данные
1		

на основании следующих документов:

_____
(перечень документов)

_____

_____

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение № 9 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 555

Форма уведомления субъекта персональных данных о невозможности прекращения обработки и уничтожения персональных данных

В соответствии с ч.3, ч.4, ч.5 ст. 21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»

Кому: _____

_____

Адрес: _____

_____

УВЕДОМЛЕНИЕ

О невозможности прекращения обработки и уничтожения персональных данных

Уважаемый (ая) _____,

уведомляем Вас о том, что оператор персональных данных ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), юридический адрес: 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, руководствуясь: _____

(правовое основание обработки персональных данных)

_____

осуществляет обработку Ваших персональных данных, а именно:

№ п.п.	Персональные данные
1	Пример: Иванов Иван Иванович 1975 г.р.

в целях:

_____

(цель обработки персональных данных)

_____

_____ о _____

(дата начала обработки) (дата конца обработки)

Обработка указанных персональных данных не может быть прекращена в связи с

_____

(причина окончания обработки персональных данных)

По окончании обработки Ваши персональные данные будут уничтожены.

_____ _____ _____

(должность) (Ф.И.О.) (подпись)

Приложение № 10 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 353

Форма уведомления субъекта персональных данных о прекращении обработки и уничтожении его персональных данных

В соответствии с ч.3, ч.4, ч.5 ст. 21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»

Кому: _____

_____

Адрес: _____

_____

УВЕДОМЛЕНИЕ

О прекращении и уничтожении персональных данных

Уважаемый (ая) _____,

уведомляем Вас о том, что оператор персональных данных ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), юридический адрес: 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, руководствуясь: _____
(правовое основание обработки персональных данных)

_____

осуществлял обработку Ваших персональных данных, а именно:

№ п.п.	Персональные данные
1	Пример: Иванов Иван Иванович 1975 г.р.

в целях:

_____
(цель обработки персональных данных)

_____

_____ о _____
(дата начала обработки) (дата конца обработки)

Обработка указанных персональных данных была прекращена в связи с

_____
(причина окончания обработки персональных данных)

По окончании обработки Ваши персональные данные были уничтожены.

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение № 11 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 325

Форма уведомления субъекта персональных данных о внесении изменений в его персональные данные

В соответствии с ч.3 ст.20 и ч.2 ст.21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»

Кому: _____

_____

Адрес: _____

_____

УВЕДОМЛЕНИЕ

О внесении изменений в персональные данные

Уважаемый (ая) _____,

уведомляем Вас о том, что оператор персональных данных ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), юридический адрес: 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, внес следующие изменения в Ваши персональные данные:

п.п.	Исходные данные	Новые данные
.		

на основании следующих документов:

_____
(перечень документов)

_____

_____

_____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение № 12 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Соглашение о неразглашении персональных данных работника

Я, _____
(фамилия, имя, отчество, должность)

в качестве работника ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ) в период трудовых / договорных отношений с ФГБОУ ВО РГСУ и по их окончании обязуюсь:

1. Не раскрывать конфиденциальную информацию, содержащую персональные данные, к которым я буду допущен или которые станут известны мне в процессе трудовой деятельности.
2. Не передавать третьим лицам и не раскрывать публично персональные данные без согласия ФГБОУ ВО РГСУ.
3. Выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению безопасности персональных данных.
4. В случае попытки посторонних лиц получить от меня конфиденциальную информацию, содержащую персональные данные, немедленно сообщить об этом своему непосредственному руководителю.
5. Сохранять конфиденциальность персональных данных, полученных ФГБОУ ВО РГСУ от третьих лиц, с которыми ФГБОУ ВО РГСУ имеет деловые отношения.
6. Не использовать информацию, содержащую персональные данные, для извлечения личной выгоды, а также в целях, которые могут нанести ущерб ФГБОУ ВО РГСУ, субъектам персональных данных, либо иным лицам.
7. В случае моего увольнения все материальные носители персональных данных, которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в ФГБОУ ВО РГСУ передать моему непосредственному руководителю.
8. Об утрате или недостаче материальных носителей персональных данных, удостоверений, пропусков, ключей от защищаемых помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к раскрытию конфиденциальной информации, содержащей персональные данные, а также о причинах и условиях возможного раскрытия персональных данных немедленно сообщать моему непосредственному руководителю и Ректору.

До моего сведения доведено с разъяснениями Положение об обработке персональных данных.

Я понимаю, что во время исполнения своих должностных обязанностей, мне приходится заниматься обработкой персональных данных. Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный. В связи с этим, даю обязательство, при обработке персональных данных соблюдать все описанные в «Положении об обработке персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения, составляющие персональные данные. Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я могу быть привлечен(а) к дисциплинарной и материальной ответственности в порядке, установленном в Трудовом кодексе РФ и иными федеральными законами, а также привлечен(а) к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Один экземпляр
соглашения получил

_____ _____
(подпись) (подпись)

«___»_____20_ г. «___»_____20_ г.

Приложение № 13 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Шаблон поручения об изменении персональных данных

_____
(Ф.И.О.)
_____
(должность)

ПОРУЧЕНИЕ
№___
Об изменении персональных данных

г. Москва «___» _____ 20__ года

В связи с обращением субъекта персональных данных/ его законного представителя/ государственного надзорного органа, на основании ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ

ПРОШУ:

1. В срок до _____ произвести изменение персональных данных:

№ п.п.	Персональные данные
1.	Пример: Иванов Иван Иванович 1975 г.р.

Новыми персональными данными:

№ п.п.	Персональные данные
1.	Пример: Петров Иван Иванович 1975г.р.

Ответственный: _____

Принято к исполнению: _____ _____ _____
(Ф.И.О.) (подпись) (дата)

2. Контроль за исполнением возложить на: _____

ОТЧЕТ:

Персональные данные субъекта ___Иванова И.И.____ изменены.

Выполнил: _____ _____ _____
(должность) (Ф.И.О.) (подпись)

Работу принял: _____ _____ _____
(должность) (Ф.И.О.) (подпись)

Приложение № 14 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» сентября 2020 г.
№ 356

Уведомление субъекта персональных данных

«___» _____ ____ г.

Уважаемый(ая),_____,
(Ф.И.О.)

на основании Договора № _____ от __.__.20__г. ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), адрес места нахождения: 129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, получил от

_____
_____
_____ (наименование организации, с указанием адреса, от которой получены персональные данные субъекта) следующую информацию, содержащую Ваши персональные данные:

_____,
(перечислить)

Указанная информация будет обработана и использована оператором (ФГБОУ ВО РГСУ) в целях:

-

_____.

Пользователями Ваших персональных данных будут являться работники ФГБОУ ВО РГСУ» и/или юридическое лицо, состоящее в договорных отношениях с ФГБОУ ВО РГСУ.

Уведомляем Вас, что Вы вправе:

- получать в доступной форме сведения об операторе; о наличии у оператора персональных данных, идентифицирующих Вас как субъекта персональных данных, подтверждение факта обработки персональных данных, а также на ознакомление с такими данными в случаях, прямо предусмотренных законом;
- обжаловать действия или бездействия оператора персональных данных в уполномоченный орган или в судебном порядке;
- защищать свои права и законные интересы, в том числе требовать возмещения убытков и компенсации морального вреда, в суде;
- в любой момент отозвать согласие на обработку Ваших персональных данных.
- уточнить правовые основания и цели обработки персональных данных;
- уточнить цели и применяемые оператором способы обработки персональных данных;
- уточнить наименование и место нахождения оператора, сведения о лицах, за исключением работников оператора, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором;
- уточнить сроки обработки персональных данных, в том числе сроки их хранения;
- уточнить порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- уточнить наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- заявить возражения против решения оператора персональных данных, принятого оператором персональных данных на основании исключительно автоматизированной обработки персональных данных, (при этом о результатах рассмотрения возражений оператор

персональных данных должен уведомить субъекта персональных данных в течение 30 рабочих дней с момента получения возражений).

_____

(должность, подпись, Ф.И.О. работника ФГБОУ ВО РГСУ)

_____

(дата)

Настоящее уведомление получил

_____

(подпись, Ф.И.О. субъекта персональных данных)

_____

(дата)

Приложение № 15 к Положению об обработке персональных данных в РГСУ, утвержденному приказом РГСУ
от «16» марта 2020 г.
№ 355

Согласие на обработку персональных данных пользователя гостиничных услуг

Я,_____, паспорт серии _____, номер _____, выданный _____ «___»_____ _____ года, проживающий(ая) по адресу: _____, в соответствии с Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных» даю согласие ФГБОУ ВО «Российский государственный социальный университет» (ФГБОУ ВО РГСУ), зарегистрированному по адресу129226, г. Москва, ул. Вильгельма Пика, дом 4, стр.1, на обработку моих персональных данных, а именно:

- фамилия, имя, отчество, число, месяц, год рождения;
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- номер контактного телефона;
- адрес электронной почты;
- данные о месте работы (при бронировании командируемых юридических лиц и ИП);
- номер банковской карты (в случае оплаты гостиничных услуг таковой).

Целью обработки персональных данных является оказание гостиничных услуг.

Настоящее согласие предоставляется на совершение следующих действий (операций) с моими персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), предоставление (работникам ФГБОУ ВО РГСУ, сотрудникам Федеральной таможенной службы РФ, сотрудникам МВД РФ), использование, блокирование, удаление, уничтожение, осуществляемых как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

Персональные данные будут обрабатываться в течение времени моего проживания в гостинице (129226, г. Москва, ул. Вильгельма Пика, дом 4, стр. 1), а также в течение одного года после моего выезда из гостиницы

Я подтверждаю, что ознакомлен(а) с требованиями законодательства Российской Федерации, устанавливающими порядок обработки персональных данных, с политикой ФГБОУ ВО РГСУ в отношении обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания на период не менее чем срок хранения документов, установленных архивным законодательством.

Я подтверждаю, что мне известно о праве отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес оператора. В случае моего отзыва согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ согласно части 2 статьи 9 «О персональных данных».

«__» _____ 20__ г. _____ (_____)
(подпись, расшифровка подписи)

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Кадры»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Починок Н.Б.

«__»_____20__г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20___г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV. 8 (495) 221-21-41 ARinteg@ARinteg.ru
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю». 8 (812) 407-34-71 Spb@ARinteg.ru
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44. 8 (343) 247-83-68 Ural@ARinteg.ru
www.ARinteg.ru @arinteg2018 www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО « РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных в ФГБОУ ВО «РГСУ», послужит основой для проведения мероприятий по классификации информационной системы персональных данных в ФГБОУ ВО «РГСУ», проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн Организации, и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн Организации.

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Кадры» в составе:

- «1С: Управление образовательным процессом»;
- «1С: Зарплаты и кадры государственного учреждения 3.0»;
- «1С: Бухгалтерия государственного учреждения 2.0»;
- «1С: Зарплаты и кадры бюджетного учреждения 1.0»;
- «1С: Бухгалтерия государственного учреждения 1.0»;
- «1С: Розница»;
- «1С: Документооборот»;
- «Система дистанционного обучения»;
- «Веб-сайт»;
- Корпоративная почта;
- Корпоративный портал;
- «1С: Государственные муниципальные закупки»;
- «1С: Планово-финансовое управление».

Характеристики ИСПДн «Кадры» представлены в Таблице 1:

Таблица 1. Характеристики ИСПДн «Кадры»

Характеристика	Значение
Категория обрабатываемых персональных данных	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационного обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. N 1119), для ИСПДн «Кадры» актуальны угрозы 3-го типа и информационная система обрабатывает иные персональные данные менее, чем 100.000 субъектов, являющихся работниками оператора **необходимо обеспечение 4-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;

- «Базовая модель» угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Приказ ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02. 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Кадры» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок;

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Кадры», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Кадры».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Кадры».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Кадры».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн Организации в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Кадры» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Кадры».

В ИСПДн «Кадры» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Кадры» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Кадры»

Уязвимость ИСПДн «Кадры» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;
- неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.п.);
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Кадры» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.,
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических

переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Кадры», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Кадры»

Для ИСПДн «Кадры» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

- угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Кадры». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;
- угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн «Кадры»

Таблица 3. Показатели исходной защищенности ИСПДн «Кадры»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн«Кадры» без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «**средний**», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: **Y1 = 5.**

4.4. Определение вероятности реализации угроз в ИСПДн «Кадры»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Кадры» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Кадры» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором ведется	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1−Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
обработка персональных данных					
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного доступа к системе по беспроводным каналам	5	0,5	Средняя	Средняя	Неактуально
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,15	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0.5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0.35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой	5	0,5	Высокая	Средняя	Актуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
информации					
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0.5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Кадры» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза несанкционированного воздействия на средство защиты информации
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.
- Угроза выхода процесса за пределы виртуальной машины
- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- Несанкционированное отключение средств защиты
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками

- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неполтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Кадры»

На основании назначения ИСПДн «Кадры» к нарушителям информационной безопасности ИСПДн «Кадры» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);
б. бывшие работники (пользователи);
в. пользователи информационной системы;
г. администраторы информационной системы и администраторы безопасности;
д. преступные группы

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Кадры»исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – д) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Кадры», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Кадры» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Кадры» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Кадры»приведен в Таблице 4.

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	**Категория нарушителя:**	
	Категория I	**Категория II**
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1. Зарегистрированные пользователи ИСПДн Организации (пользователи,

		администраторы); 2. Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств, не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Кадры».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «Кадры», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Кадры», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Кадры», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;
- преступные группы (криминальные структуры);

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Кадры», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;

• техническими и программными средствами, аналогичным средствам ИСПДн «Кадры», включая соответствующие средства каналообразования, маршрутизации и т.д.;

• техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Кадры»;

• специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

• проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Кадры»;

• проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Кадры»;

• проводить попытки навязывания ложной информации;

• внедрять вредоносное ПО;

• проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «Кадры».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн Организации.

5.2. Внутренние нарушители «Кадры»

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Кадры»:

• зарегистрированные пользователи ИСПДн «Кадры»;

• администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

• работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;

• несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;

• легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Кадры», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к

ресурсам ИСПДн Организации, а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Сотрудник «Кадры», не являющийся зарегистрированным пользователем ИСПДн Организации, но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов Организации, имеющий доступ в помещения, где установлено оборудование ИСПДн «Кадры».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

- располагать именами (логинами) зарегистрированных пользователей ИСПДн, а также вести разведку паролей зарегистрированных пользователей;
- иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Кадры» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);
- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Кадры»

Зарегистрированный пользователь ИСПДн «Кадры» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких

пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Кадры», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;

- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2			
Н3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер	Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
Н4			
Н5			
Н6	Располагают любыми аппаратными		

	компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «Кадры» подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Кадры»

Вид нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа к контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн «Кадры» (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi ($1 \leq i \leq 5$), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн «Кадры» по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровня защиты от НСД к ПДн
ИСПДн «Кадры»	H2	АК2

5.4. Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Кадры» соответствуют возможностям нарушителя типа H1 и H2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 г № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн,

обрабатываемых в ИСПДн «Кадры», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.5. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Кадры» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 № 1119 можно сделать вывод, что для ИСПДн «Кадры» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Кадры», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Обучающиеся»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Пс чинок Н.Б.

«__» _____ 20__ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__» _____ 20__ г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю».
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44
8 (495) 221-21-41
8 (812) 407-34-71
8 (343) 247-83-68
ARinteg@ARinteg.ru
Spb@ARinteg.ru
Ural@ARinteg.ru
www.ARinteg.ru
@arinteg2018
www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных, послужит основой для проведения мероприятий по классификации информационной системы персональных данных, проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

В настоящем документе используются следующие обозначения и их сокращения:

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система «Обучающиеся», обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн «Обучающиеся», и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн «Обучающиеся».

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Обучающиеся» в составе:

- «1С: Управление образовательным процессом»;
- «1С: Зарплаты и кадры государственного учреждения 3.0»;
- «1С: Бухгалтерия государственного учреждения 2.0»;
- «1С: Зарплаты и кадры бюджетного учреждения 1.0»;
- «1С: Бухгалтерия государственного учреждения 1.0»;
- «1С: Библиотека»;
- «1С: Документооборот»;
- «Система дистанционного обучения»;
- «Портфолио»
- «Веб-сайт»;
- «1С: Конвертер «Московский социальный регистр»
- Корпоративный портал;

Характеристики ИСПДн «Обучающиеся» представлены в Таблице 1.

Таблица 1. Характеристики ИСПДн «Обучающиеся»

Характеристика	Значение
Категория обрабатываемых персональных данных	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	более 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и/или сетям международного информационного обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. N 1119), для ИСПДн «Обучающиеся» актуальны угрозы 3-го типа и информационная система обрабатывает иные персональные данные более, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 3-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 года;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 года;
- Приказ ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства от 01.11.2012. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Обучающиеся» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН);

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Обучающиеся», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Обучающиеся».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Обучающиеся».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Обучающиеся».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн «Обучающиеся» в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Обучающиеся» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн Организации.

В ИСПДн «Обучающиеся» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Обучающиеся» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для

осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Обучающиеся»

Уязвимость ИСПДн «Обучающиеся» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;
- неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия),
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Обучающиеся» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

• функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

• функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Обучающиеся», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;

• отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Обучающиеся»

Для ИСПДн «Обучающиеся» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

• угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Обучающиеся». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;

• угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

• угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их

обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14 февраля 2008 года.

4.3.1. Определение уровня исходной защищенности ИСПДн «Обучающиеся»

Таблица 3. Показатели исходной защищенности ИСПДн «Обучающиеся»

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	Низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «средний», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент:

Y1 = 5

4.4. Определение вероятности реализации угроз в ИСПДн «Обучающиеся»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Обучающиеся» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Обучающиеся» и перечня актуальных угроз безопасности

Наименование угрозы	**Коэф. опред. Вероятность наступления угрозы (Y2)**	**Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)**	**Возможность реализации угрозы**	**Опасность угрозы (К3)**	**Актуальность угрозы**
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка	2	0,35	Низкая	Средняя	Неактуально

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
персональных данных					
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Просмотр информации с помощью специальных электронных устройств внедренных в помещения, в котороч ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0.5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного доступа к системе по	5	0.5	Средняя	Средняя	Неактуально

Наименование угрозы	Коэф. опред. Вероятности наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
беспроводным каналам					
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программы	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за неналежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально

Наименование угрозы	Коэф. опред. Вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0,5	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0,5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Обучающиеся» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза несанкционированного воздействия на средство защиты информации
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.
- Угроза выхода процесса за пределы виртуальной машины

- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- Несанкционированное отключение средств защиты
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Обучающиеся»

На основании назначения ИСПДн «Обучающиеся» к нарушителям информационной безопасности ИСПДн «Обучающиеся» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);
б. бывшие работники (пользователи);
в. пользователи информационной системы;
г. администраторы информационной системы и администраторы безопасности;
д. преступные группы

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн «Обучающиеся», в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации (далее - СКЗИ) и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Обучающиеся» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – д) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Обучающиеся», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Обучающиеся» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Обучающиеся» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Обучающиеся» приведен в Таблице 4.

Таблица 4. Виды и категории нарушителей безопасности ПДн «Обучающиеся»

Вид нарушителя	**Категория нарушителя**	
	Категория I	**Категория II**
Внешние	1 Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1 зарегистрированные пользователи ИСПДн «Обучающиеся» (пользователи, администраторы); 2 незарегистрированные пользователи ИСПДн «Обучающиеся», но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее - СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Обучающиеся».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн Организации, находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Обучающиеся», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Обучающиеся», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;
- преступные группы (криминальные структуры);

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Обучающиеся», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «Обучающиеся», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Обучающиеся»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Обучающиеся»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Обучающиеся»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн Организации.

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн Организации.

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Обучающиеся»:

- зарегистрированные пользователи ИСПДн «Обучающиеся»;
- администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;

• легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Обучающиеся», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн Организации, а так же контроль за порядком обращения конфиденциальной информации.

5.2.1. Работник Организации, не являющийся зарегистрированным пользователем ИСПДн «Обучающиеся», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов Организации, имеющий доступ в помещения, где установлено оборудование ИСПДн «Обучающиеся».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

• располагать именами (логинами) зарегистрированных пользователей ИСПДн, а также вести разведку паролей зарегистрированных пользователей;

• иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Обучающиеся» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

• подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);

• получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;

- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Обучающиеся»

Зарегистрированный пользователь ИСПДн «Обучающиеся» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Обучающиеся», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2			
Н3	Дополнительные возможности по получению		
Н4			

H5	аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер	Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
H6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «Обучающиеся» подразделяются на следующие категории и типы, которые представлены в Таблице 7.

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Обучающиеся»

Вид нарушителя	**Категория нарушителя**		**Тип нарушителя**
	Категория I	**Категория II**	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн «Обучающиеся» (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн «Обучающиеся», но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi (1 включают в себя возможности нарушителя Hi (1≤ i ≤5), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн «Обучающиеся» по уровням защиты от НСД к ПДн

ИСПДн Организации	**Тип нарушителя**	**Уровни защиты от НСД к ПДн**
ИСПДн «Обучающиеся»	H2	АК2

Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Обучающиеся» соответствуют возможностям нарушителя типа H1 и H2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской

Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432. криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Обучающиеся», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.4. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Обучающиеся» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 №1119 можно сделать вывод, что для ИСПДн «Обучающиеся» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Обучающиеся», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Абитуриенты»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Починок Н.Б.

«__» _____ 20__ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__» _____ 20__ г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV. 8 (495) 221-21-41 ARinteg@ARinteg.ru
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю». 8 (812) 407-34-71 Spb@ARinteg.ru
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44. 8 (343) 247-83-68 Ural@ARinteg.ru
www.ARinteg.ru @arinteg2018 www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системе персональных данных в ФГБОУ ВО «РГСУ», послужит основой для проведения мероприятий по классификации информационной системе персональных данных в ФГБОУ ВО «РГСУ», проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн Организации, и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн Организации.

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн «Абитуриенты»

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Абитуриенты» в составе:

- «1С: Документооборот»;
- «Веб-сайт»;

Характеристики ИСПДн «Абитуриенты» представлены в Таблице 1.

Таблица 1. Характеристики ИСПДн «Абитуриенты».

Характеристика	Значение
Категории обрабатываемых персональных данных	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	более 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. N 1119), для ИСПДн «Абитуриенты» актуальны угрозы 3-го типа и информационная система обрабатывает иные персональные данные более, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 3-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств

криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;

- Постановление Правительства от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Абитуриенты» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН),

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Абитуриенты», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространиться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Абитуриенты».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Абитуриенты».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и

электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Абитуриенты».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн «Абитуриенты» в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Абитуриенты» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Абитуриенты».

В ИСПДн Организации угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Абитуриенты» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Абитуриенты»

Уязвимость ИСПДн «Абитуриенты» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;

• преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;

• неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;

• несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);

• сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

• уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

• уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

• в микропрограммах, в прошивках запоминающих устройств;

• в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Абитуриенты» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;

• в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);

• в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

• функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

• отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные

платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Абитуриенты», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Абитуриенты»

Для ИСПДн «Абитуриенты» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

- угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Абитуриенты». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;
- угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн «Абитуриенты»

Таблица 3. Показатели исходной защищенности ИСПДн «Абитуриенты»

Технические и эксплуатационные характеристики ИСПДн «Абитуриенты»	**Уровень защищенности**
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий

Технические и эксплуатационные характеристики ИСПДн «Абитуриенты»	Уровень защищенности
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	Низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «средний», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент:

$$Y1 = 5$$

4.4. Определение вероятности реализации угроз в ИСПДн «Абитуриенты»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Абитуриенты» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Абитуриенты» и перечня актуальных угроз безопасности

Наименование угрозы	Коэффициент, определяющий вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэффициент, определяющий вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
персональных данных					
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного доступа к системе по беспроводным каналам	5	0,5	Средняя	Средняя	Неактуально
Угрозы некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально

Наименование угрозы	Коэффициент, определяющий вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1−Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Нелекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0,5	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтвержденного ввода данных оператором в систему, связанную с	0	0,25	Высокая	Средняя	Актуально

Наименование угрозы	Коэффициент, определяющий вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
безопасностью					
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0.5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Абитуриенты» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза несанкционированного воздействия на средство защиты информации
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.
- Угроза выхода процесса за пределы виртуальной машины
- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- Несанкционированное отключение средств защиты
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Абитуриенты»

На основании назначения ИСПДн «Абитуриенты» к нарушителям информационной безопасности ИСПДн «Абитуриенты» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);
б. бывшие работники (пользователи);
в. пользователи информационной системы;
г. администраторы информационной системы и администраторы безопасности;
д. преступные группы

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации (далее - СКЗИ) и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Абитуриенты»исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) - д) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Абитуриенты», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Абитуриенты» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Абитуриенты» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Абитуриенты» приведен в Таблице 4.

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	Категории нарушителя	
	Категория I	**Категория II**
Внешние	1 Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1- зарегистрированные пользователи ИСПДн «Абитуриенты» (пользователи, администраторы); 2- незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;

- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее - СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Абитуриенты».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «Абитуриенты», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Абитуриенты», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Абитуриенты», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;
- преступные группы (криминальные структуры);

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Абитуриенты», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичными средствам ИСПДн «Абитуриенты», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Абитуриенты»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Абитуриенты»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Абитуриенты»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «Абитуриенты».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «Абитуриенты».

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Абитуриенты»:

- зарегистрированные пользователи ИСПДн;
- администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;
- легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Абитуриенты», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «Абитуриенты», а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Работник Организации, не являющийся зарегистрированным пользователем ИСПДн «Абитуриенты», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов Организации, имеющий доступ в помещения, где установлено оборудование ИСПДн «Абитуриенты».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

- располагать именами (логинами) зарегистрированных пользователей ИСПДн, а также вести разведку паролей зарегистрированных пользователей;
- иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Абитуриенты» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя),
- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Абитуриенты»

Зарегистрированный пользователь ИСПДн «Абитуриенты» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких

пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Абитуриенты», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;

- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
H1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
H2			
H3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер	Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
H4			
H5			
H6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «Абитуриенты»подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Абитуриенты»

Вид нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн «Абитуриенты» (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi (1≤ i ≤5), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн «Абитуриенты» по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровни защиты от НСД к ПДн
ИСПДн «Абитуриенты»	Н2	АК2

Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Абитуриенты» соответствуют возможностям нарушителя типа Н1 и Н2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Абитуриенты», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.4. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Абитуриенты» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 № 1119 можно сделать вывод, что для ИСПДн «Абитуриенты» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при

проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Абитуриенты», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учрежденне высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Контрагенты»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Починок Н.Б.

«__»_____20__ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20__ г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV. 8 (495) 221-21-41 ARinteg@ARinteg.ru
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю». 8 (812) 407-34-71 Spb@ARinteg.ru
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44. 8 (343) 247-83-68 Ural@ARinteg.ru
www.ARinteg.ru @arinteg2018 www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системе персональных данных в ФГБОУ ВО, послужит основой для проведения мероприятий по классификации информационной системе персональных данных в ФГБОУ ВО, проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система «Контрагенты», обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн «Контрагенты», и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн «Контрагенты».

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн «Контрагенты»

При проведении обследовании ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Контрагенты» в составе:

- «1С: Отель»;
- «1С: Розница»;
- «1С: Документооборот»;
- «Веб-сайт»;
- «Корпоративная почта»

Характеристики ИСПДн «Контрагенты» предоставлены в Таблице 1:

Таблица 1. Характеристики ИСПДн «Контрагенты»

Характеристика	Значение
Категория обрабатываемых персональных данных	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и/или сетям международного информационно обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01 ноября 2012 г. № 1119), для ИСПДн «Контрагенты» актуальны угрозы 3-го типа и информационная система обрабатывает иные персональные данные более, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 4-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Приказ ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Контрагенты» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН);

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Контрагенты», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Контрагенты».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Контрагенты».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Контрагенты».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн «Контрагенты» в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Контрагенты» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Контрагенты».

В ИСПДн «Контрагенты» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Контрагенты» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются

с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Контрагенты»

Уязвимость ИСПДн «Контрагенты» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;
- неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Контрагенты» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

• отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

• функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

• функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Контрагенты», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;

• отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Контрагенты»

Для ИСПДн «Контрагенты» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

• угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Контрагенты». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;

• угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн «Контрагенты»

Таблица 3. Показатели исходной защищенности ИСПДн «Контрагенты»

Технические и эксплуатационные характеристики ИСПДн «Контрагенты»	Уровень защищенности
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «средний», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: **Y1 = 5**

4.4. Определение вероятности реализации угроз в ИСПДн Организации

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Контрагенты» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Контрагенты» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0.35	Средняя	Низкая	Неактуально

Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально

Угроза несанкционированного доступа к системе по беспроводным каналам	5	0,5	Средняя	Средняя	Неактуально
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за неналежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально

Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0,5	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0.5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Контрагенты» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза несанкционированного воздействия на средство защиты информации
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.
- Угроза выхода процесса за пределы виртуальной машины

- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- Несанкционированное отключение средств защиты
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Контрагенты»

На основании назначения ИСПДн «Контрагенты» к нарушителям информационной безопасности ИСПДн «Контрагенты»следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);
б. бывшие работники (пользователи);
в. пользователи информационной системы;
г. администраторы информационной системы и администраторы безопасности;
д. преступные группы

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации (далее - СКЗИ) и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Контрагенты» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – д) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Контрагенты», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Контрагенты» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Контрагенты» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Контрагенты» приведен в Таблице 4.

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	Категория нарушителя	
	Категория I	Категория II
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону.	
Внутренние		1. Зарегистрированные пользователи ИСПДн «Контрагенты» (пользователи, администраторы). 2. Незарегистрированные пользователи ИСПДн«Контрагенты», но имеющие право доступа в контролируемую зону.

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее - СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Контрагенты».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «Контрагенты», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Контрагенты», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Контрагенты», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;
- преступные группы (криминальные структуры);

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными

фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Контрагенты», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «Контрагенты», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Контрагенты»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Контрагенты»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Контрагенты»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн Организации.

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «Контрагенты».

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Контрагенты»:

- зарегистрированные пользователи ИСПДн «Контрагенты»;
- администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;
- легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Контрагенты», и к информационным ресурсам ИСПДн «Контрагенты» исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа

в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «Контрагенты», а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Сотрудник Организации, не являющийся зарегистрированным пользователем ИСПДн «Контрагенты», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов Организации, имеющий доступ в помещения, где установлено оборудование ИСПДн «Контрагенты».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

- располагать именами (логинами) зарегистрированных пользователей ИСПДн «Контрагенты», а также вести разведку паролей зарегистрированных пользователей;
- иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Контрагенты» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);
- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;

- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Контрагенты»

Зарегистрированный пользователь ИСПДн «Контрагенты» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объему ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Контрагенты», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2			
Н3	Дополнительные возможности по получению аппаратных компонент		
Н4			
Н5		Возможности по	Могут проводить

	криптосредства и СФК зависят от реализованных в информационной системе организационных мер	использованию штатных средств зависят от реализованных в информационной системе организационных мер	лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
Н6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «Контрагенты» подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Контрагенты»

Тип нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн Организации (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi (1≤ i ≤5), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн Организации по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровни защиты от НСД к ПДн
ИСПДн «Контрагенты»	H2	АК2

Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Контрагенты» соответствуют возможностям нарушителя типа H1 и H2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке

персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 г № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Контрагенты», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.4. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Контрагенты» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 №1119 можно сделать вывод, что для ИСПДн «Контрагенты» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Контрагенты», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Медицина»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Почивок Н.Б.

«__»_____20__ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20__ г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV. 8 (495) 221-21-41 ARinteg@ARinteg.ru
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю». 8 (812) 407-34-71 Spb@ARinteg.ru
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44. 8 (343) 247-83-68 Ural@ARinteg.ru
www.ARinteg.ru @arinteg2018 www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных, послужит основой для проведения мероприятий по классификации информационной системы персональных данных, проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн «Медицина», и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн .

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Медицина» в составе:

- «1С: Документооборот»;
- Корпоративная почта;
- МИС «МЕДИАЛОГ»;
- МИС «Инфоклиника».

Характеристики ИСПДн «Медицина» представлены в Таблице 1:

Таблица 1. Характеристики ИСПДн «Медицина»

Характеристика	Значение
Категория обрабатываемых персональных данных	Специальные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01 ноября 2012 г. № 1119), для ИСПДн «Медицина» актуальны угрозы 3-го типа и информационная система обрабатывает специальные персональные данные менее, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 3-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.;

- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02. 2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Медицина» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН);

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Медицина», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Медицина».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Медицина».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Медицина».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн «Медицина» в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Медицина» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информация, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Медицина».

В ИСПДн «Медицина» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Медицина» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Медицина»

Уязвимость ИСПДн «Медицина» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

• ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;

• преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;

• неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;

• несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);

• сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

• уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

• уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

• в микропрограммах, в прошивках запоминающих устройств;

• в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Медицина» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;

• в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);

• в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

• функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

• отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Медицина», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Медицина»

Для ИСПДн «Медицина» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

- угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Медицина». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;
- угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн

Таблица 3. Показатели исходной защищенности ИСПДн «Медицина»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	Низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «**средний**», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: **Y1 = 5**

4.4. Определение вероятности реализации угроз в ИСПДн «Медицина»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн Организации в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Медицина» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных					
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Высокая	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Высокая	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Высокая	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Высокая	Актуально
Угрозы внедрения вредоносного ПО	5	0.5	Высокая	Высокая	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Высокая	Актуально
Угрозы фишинга	5	0,5	Высокая	Высокая	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Высокая	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокая	Высокая	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокая	Средняя	Актуально
Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокая	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокая	Средняя	Актуально
«Отказ в обслуживании»	2	0,35	Высокая	Низкая	Актуально
Угроза внедрения вредоносного кода в BIOS	5	0,5	Высокая	Высокая	Неактуально
Угроза изменения режимов работы аппаратных элементов	5	0,5	Высокая	Средняя	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угроза несанкционированного удаленного внеполосного доступа	5	0,5	Высокая	Высокая	Неактуально
Угроза эксплуатации шифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0.5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	5	0,5	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0,5	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0,5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Медицина» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору
- Угроза выхода процесса за пределы виртуальной машины
- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- «Отказ в обслуживании»
- Несанкционированное отключение средств защиты
- Компьютерные вирусы

- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Медицина»

На основании назначения ИСПДн «Медицина» к нарушителям информационной безопасности ИСПДн «Медицина» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);

б. бывшие работники (пользователи);

в. Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

г. лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ;

д. пользователи информационной системы;

е. администраторы информационной системы и администраторы безопасности;

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации (далее – «СКЗИ») и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Медицина» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – е) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Медицина», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Медицина» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Медицина» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Медицина» приведен в Таблице 4:

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	**Категории нарушителя**	
	Категория I	**Категория II**
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1. зарегистрированные пользователи ИСПДн «Медицина» (пользователи, администраторы); 2. незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее - СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Медицина».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «Медицина», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Медицина», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Медицина», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Медицина», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «Медицина», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Медицина»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Медицина»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Медицина»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «Медицина».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «Медицина».

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Медицина»:

- зарегистрированные пользователи ИСПДн «Медицина»;
- администраторы информационных систем и администраторы безопасности;
- лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора;
- лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ.

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;
- легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Медицина», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «Медицина», а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Сотрудник внешней организации, не являющийся зарегистрированным пользователем ИСПДн «Медицина», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Данный вид нарушителя характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относятся лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных работ, имеющие доступ в помещения, где установлено оборудование ИСПДн «Медицина».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Медицина» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Медицина»

Зарегистрированный пользователь ИСПДн «Медицина» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за

выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Медицина» и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Сферы информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2		Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
Н3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер		
Н4			
Н5			
Н6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн Организации подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Медицина»

Вид нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн Организации (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi ($1 \leq i \leq 5$), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн Организации по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровни защиты от НСД к ПДн
ИСПДн «Медицина»	H2	АК2

Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Медицина» соответствуют возможностям нарушителя типа H1 и H2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 г № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Медицина», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.4. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Медицина» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 № 1119 можно сделать вывод, что для ИСПДн «Медицина» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Медицина», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «СКУД»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Гончинок Н.Б.

«__»_____20___ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20___ г.

"АРинтег"

Москва, 2018 г.

ООО «АРинтег»
105005, г. Москва, ул. Радио, д. 24, корп. 1, помещение IV. 8 (495) 221-21-41 ARinteg@ARinteg.ru
195027, г. Санкт-Петербург, пр. Шаумяна, д. 8, корп. 1, литера «Ю». 8 (812) 407-34-71 Spb@ARinteg.ru
620026, г. Екатеринбург, Свердловская область, ул. Куйбышева, д. 44. 8 (343) 247-83-68 Ural@ARinteg.ru
www.ARinteg.ru @arinteg2018 www.facebook.com/ARinteg/

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Тераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных, послужит основой для проведения мероприятий по классификации информационной системы персональных данных, проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на подлержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн «СКУД», и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн «СКУД».

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

Характеристики ИСПДн «СКУД»

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «СКУД» в составе:

- ИС «PERCo»

Характеристики ИСПДн «СКУД» представлены в Таблице 1:

Таблица 1. Характеристики ИСПДн «СКУД»

Характеристика	Значение
Категория обрабатываемых персональных данных	Биометрические персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	Без подключения

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01 ноября 2012 г. № 1119), для ИСПДн «СКУД» актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные менее, чем 100.000 субъектов, являющихся работниками оператора **необходимо обеспечение 3-го уровня защищенности.**

Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных

Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;

- Постановление Правительства от 01.11.2012. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификации угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «СКУД» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН);

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа в ИСПДн «СКУД», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «СКУД».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «СКУД».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «СКУД».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн Организации в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «СКУД» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн Организации.

В ИСПДн «СКУД» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн Организации с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «СКУД»

Уязвимость ИСПДн «СКУД» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;

• неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;

• несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);

• сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

• уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

• уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

• в микропрограммах, в прошивках запоминающих устройств;

• в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «СКУД» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;

• в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);

• в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

• функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;

• отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «СКУД», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «СКУД»

Для ИСПДн Организации можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

- угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «СКУД». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;
- угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.2.5. Определение уровня исходной защищенности ИСПДн «СКУД»

Таблица 3. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «**средний**», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент:

Y1 = 5

Определение вероятности реализации угроз в ИСПДн «СКУД»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «СКУД» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

Определение вероятности реализации угроз в ИСПДн «СКУД» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения, в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
персональных данных					
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Неактуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Неактуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Неактуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Неактуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Неактуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Неактуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза загрузки нештатной операционной системы	5	0,5	Высокая	Средняя	Актуально
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз техногенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молнии, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Неактуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой	5	0,5	Высокая	Средняя	Актуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
информации					
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	0	0.25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Неактуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0.5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «СКУД» являются:

- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза загрузки нештатной операционной системы
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств
- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «СКУД»

На основании назначения ИСПДн «СКУД» к нарушителям информационной безопасности ИСПДн «СКУД» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);

б. бывшие работники (пользователи);

в. лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

г. лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ;

д. пользователи информационной системы;

е. администраторы информационной системы и администраторы безопасности;

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «СКУД» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – е) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «СКУД», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «СКУД» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «СКУД» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «СКУД» приведен в Таблице 4:

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	Категория нарушителя	
	Категория I	Категория II
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1. зарегистрированные пользователи ИСПДн «СКУД» (пользователи, администраторы); 2. незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;

- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств, не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «СКУД».

Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «СКУД», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «СКУД», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «СКУД», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные сотрудники;

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные сотрудники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «СКУД», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «СКУД», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «СКУД»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «СКУД»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «СКУД»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «СКУД».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «СКУД».

Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «СКУД»:

- зарегистрированные пользователи ИСПДн «СКУД»;
- лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора;
- лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ;
- администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей,
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;
- легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «СКУД», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «СКУД», а также контроль за порядком обращения конфиденциальной информации.

5.1.2. Сотрудник Организации, не являющийся зарегистрированным пользователем ИСПДн «СКУД», но имеющий право доступа в контролируемую зону

5.1.2.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов «СКУД», имеющий доступ в помещения, где установлено оборудование ИСПДн «СКУД».

5.1.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

- располагать именами (логинами) зарегистрированных пользователей ИСПДн, а также вести разведку паролей зарегистрированных пользователей;
- иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.1.2.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.1.2.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «СКУД» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);
- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.1.3. Сотрудник внешней организации, не являющийся зарегистрированным пользователем ИСПДн «СКУД», но имеющий право доступа в контролируемую зону

5.1.3.1. Описание нарушителей (субъектов атак)

Данный вид нарушителя характеризуется тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относятся лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных работ, имеющие доступ в помещения, где установлено оборудование ИСПДн «СКУД».

5.1.3.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.1.3.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.1.3.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «СКУД» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.1.4. Зарегистрированные пользователи ИСПДн «СКУД»

Зарегистрированный пользователь ИСПДн «СКУД» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.1.4.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.1.4.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «СКУД», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.1.4.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.1.4.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения

Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2		Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	
Н3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер		
Н4			Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
Н5			
Н6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «СКУД» подразделяются на следующие категории и типы, которые представлены в Таблице 7.

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «СКУД»

Вид нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	Н1
Внутренние		1 Зарегистрированные пользователи ИСПДн Организации (пользователи)	Н2

		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi (1≤ i ≤5), и следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн Организации по уровням защиты от НСД к ПДн.

[illegible]	[illegible]	Уровни защиты от НСД к ПДн
ИСПДн «СКУД»	H2	АК2

Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «СКУД» соответствуют возможностям нарушителя типа Н1 и Н2 - соответственно, согласно классификации нарушителей, приведенной в Приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 г№ 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «СКУД», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «СКУД» лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 № 1119 можно сделать вывод, что для ИСПДн «СКУД» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «СКУД», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Отдых и проживание»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Починок Н.Б.

«__»_____20__ г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20__ г.

"АРинтег"

Москва, 2018 г.

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Телух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных в ФГБОУ ВО «РГСУ», послужит основой для проведения мероприятий по классификации информационной системы персональных данных в ФГБОУ ВО «РГСУ», проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

1. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн Организации, и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн Организации.

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Отдых и проживание» в составе:

- «1С: Отель»;
- «1С: Фитнес»;
- «Веб-сайт»;
- Корпоративный портал;
- Корпоративная почта.

Характеристики ИСПДн «Отдых и проживание» представлены в Таблице 1:

Таблица 1. Характеристики ИСПДн «Отдых и проживание»

Характеристика	Значение
Категория обрабатываемых персональных данных	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. N 1119), для ИСПДн «Отдых и проживание» актуальны угрозы 3-го типа и информационная система обрабатывает иные персональные данные менее, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 4-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 года;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 15 февраля 2008 года;

- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства №1119 от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Отдых и проживание» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок:

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Отдых и проживание», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Отдых и проживание».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Отдых и проживание».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Отдых и проживание».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн Организации в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Отдых и проживание» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Отдых и проживание».

В ИСПДн «Отдых и проживание» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Отдых и проживание» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Отдых и проживание»

Уязвимость ИСПДн «Отдых и проживание» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;
- неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Отдых и проживание» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических

переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

- функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Отдых и проживание», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционированно модифицированных функций и т.п.);
- ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Отдых и проживание»

Для ИСПДн «Отдых и проживание» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

- угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Отдых и проживание». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;
- угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности произошлось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн

Таблица 3. Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «**средний**», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: **Y1 = 5**

4.4. Определение вероятности реализации угроз в ИСПДн «Отдых и проживание»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Отдых и проживание» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Отдых и проживание» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Просмотр информации с помощью специальных электронных устройств внедренных в помещении, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза использования механизмов авторизации для повышения привилегий	2	0,35	Высокая	Средняя	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Средняя	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Средняя	Актуально
Угроза выхода процесса за пределы виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	10	1	Высокий	Средняя	Актуально
Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	10	1	Высокий	Средняя	Актуально
Угроза перехвата управления гипервизором	10	1	Высокий	Средняя	Актуально
«Отказ в обслуживании»	5	0,5	Высокая	Средняя	Актуально
Угроза несанкционированного доступа к системе по беспроводным каналам	5	0,5	Средняя	Средняя	Неактуально
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	2	0,35	Средняя	Низкая	Неактуально
Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	5	0,5	Средняя	Средняя	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	2	0,35	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Неактуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение) информации сотрудниками	5	0,5	Высокий	Средняя	Актуально
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0.5	Высокая	Средняя	Актуально
Разглашение информации,	5	0,5	Высокая	Средняя	Актуально

Наименование угрозы	Коэф. опред-вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
модификация, уничтожение сотрудниками, допущенными к ее обработке					
Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0,5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Отдых к проживание» являются:

- Угроза использования механизмов авторизации для повышения привилегий
- Угрозы, связанные с НСД к базовой системе ввода-вывода
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных
- Угрозы модификации настроек
- Угрозы внедрения вредоносного ПО
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения
- Угрозы фишинга
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- «Отказ в обслуживании»
- Угроза несанкционированного воздействия на средство защиты информации
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.
- Угроза выхода процесса за пределы виртуальной машины
- Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
- Угроза нарушения технологий обработки информации путем несанкционированного внесения изменений в образы виртуальных машин
- Угроза перехвата управления гипервизором
- Несанкционированное отключение средств защиты
- Компьютерные вирусы
- Установка ПО, не связанного с исполнением служебных обязанностей
- Угроза утраты носителей информации
- Непреднамеренная модификация (уничтожение) информации сотрудниками
- Непреднамеренное отключение средств защиты
- Выход из строя аппаратно-программных средств

- Угроза несанкционированного копирования защищаемой информации
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
- Угроза неправомерного ознакомления с защищаемой информацией
- Утечка атрибутов доступа
- Перехват за пределами контролируемой зоны

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Отдых и проживание»

На основании назначения ИСПДн «Отдых и проживание» к нарушителям информационной безопасности ИСПДн «Отдых и проживание» следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);
б. бывшие работники (пользователи);
в. пользователи информационной системы;
г. администраторы информационной системы и администраторы безопасности;
д. преступные группы

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации (далее - СКЗИ) и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Отдых и проживание» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – д) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн Организации, наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Отдых и проживание» физическими лицами (бывшими или действующими сотрудниками Организации).

Модель нарушителя информационной безопасности ИСПДн «Отдых и проживание» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Отдых и проживание» приведен в Таблице 4.

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	Категория нарушителя	
	Категория I	Категория II
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону;	
Внутренние		1. зарегистрированные

		пользователи ИСПДн «Отдых и проживание» (пользователи, администраторы); 2. незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону;

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств (далее - СФК), не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Отдых и проживание».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн Организации, находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Отдых и проживание», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн «Отдых и проживание», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- уволенные работники;
- преступные группы (криминальные структуры);

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Уволенные работники для реализации атак могут использовать свои знания о структуре сети, организации работы, защитных мерах и правах доступа и т.п.

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Отдых и проживание», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «Отдых и проживание», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Отдых и проживание»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Отдых и проживание»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Отдых и проживание»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «Отдых и проживание».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «Отдых и проживание».

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Отдых и проживание»:

- зарегистрированные пользователи ИСПДн «Отдых и проживание»;
- администраторы информационных систем и администраторы безопасности;

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

- работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;
- несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;
- легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Отдых и проживание», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн.

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «Отдых и проживание», а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Сотрудник Организации, не являющийся зарегистрированным пользователем ИСПДн «Отдых и проживание», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Внутренние нарушители характеризуются тем, что имеют практически неограниченную возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относится технический и вспомогательный персонал подразделений жизнеобеспечения объектов Организации, имеющий доступ в помещения, где установлено оборудование ИСПДн «Отдых и проживание».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут:

- располагать именами (логинами) зарегистрированных пользователей ИСПДн «Отдых и проживание», а также вести разведку паролей зарегистрированных пользователей;
- иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Отдых и проживание» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- подбора и подмены идентификатора (выдача себя за зарегистрированного пользователя);
- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Отдых и проживание»

Зарегистрированный пользователь ИСПДн «Отдых и проживание» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объему ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Отдых и проживание», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;
- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 - Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
Н1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	-
Н2			
Н3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер	Возможности по использованию штатных средств зависят от реализованных в информационной системе	
Н4			Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны
Н5			
Н6	Располагают любыми аппаратными компонентами криптосредства и СФК		

		организационных мер	информационной системы

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн Организации подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Отдых и проживание»

Вид нарушителя	Категории нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн Организации (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi ($1 \leq i \leq 5$), и следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн «Отдых и проживание» по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровни защиты от НСД к ПДн
ИСПДн «Отдых и проживание»	H2	АК2

5.4. Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Отдых и проживание» соответствуют возможностям нарушителя типа H1 и H2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных система персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Отдых и проживание», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.5. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Отдых и проживание» лиц типа И2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 № 1119 можно сделать вывод, что для ИСПДн «Отдых и проживание» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн «Отдых и проживание».

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Отдых и проживание», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

ARinteg
ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ФГБОУ ВО «РГСУ»

Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «Абилимпикс»

УТВЕРЖДАЮ

Ректор федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет»

_____ Починок Н.Б.

«__»_____20___г.

УТВЕРЖДАЮ

Генеральный директор ООО «АРинтег»

_____ Соколкова Е.А.

«__»_____20___г.

"АРинтег"

Москва, 2018 г.

ЛИСТ СОГЛАСОВАНИЯ ОТ ФГБОУ ВО «РГСУ»

Наименование организации	Должность	ФИО	Дата	Подпись
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				
ФГБОУ ВО «РГСУ»				

ЛИСТ СОГЛАСОВАНИЯ ОТ ИСПОЛНИТЕЛЯ

Наименование организации	Должность	ФИО	Дата	Подпись
ООО «АРинтег»	Руководитель отдела консалтинга и аудита	Гелух И.В.		
ООО «АРинтег»	Ведущий консультант отдела консалтинга и аудита	Гераскин И.О.		

Аннотация

Настоящий документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу интересов ФГБОУ ВО «РГСУ».

Документ предназначен для оценки реализации угроз безопасности персональных данных при их обработке в информационной системе персональных данных в ФГБОУ ВО «РГСУ». Определение перечня тех угроз и нарушителей информационной безопасности, которые являются актуальными для данных информационной системы персональных данных в ФГБОУ ВО «РГСУ», послужит основой для проведения мероприятий по классификации информационной системы персональных данных в ФГБОУ ВО «РГСУ», проектированию и внедрению системы обеспечения безопасности персональных данных в ФГБОУ ВО «РГСУ».

I. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации, а также её использования.

Защита персональных данных – комплекс мероприятий, направленных на поддержание целостности, доступности, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное средство (аппаратно-программный комплекс), реализующее контроль информации, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (Организация) – ФГБОУ ВО «РГСУ».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – система организационных и аппаратно-программных средств, обеспечивающая защиту персональных данных, обрабатываемых в информационной системе персональных данных, от уничтожения, изменения, блокирования, копирования и распространения за счет исключения несанкционированного, в том числе случайного, доступа к персональным данным.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угрозы безопасности персональных данных – 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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

ИС	Информационная система
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПЭМИН	Побочные электромагнитные излучения и наводки
ПО	Программное обеспечение
СФК	Среда функционирования криптосредств
СКЗИ	Средства криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
ФСБ России	Федеральная служба безопасности РФ
ФСТЭК России	Федеральная служба по техническому и экспортному контролю РФ

3. Объект и цели исследования

Объектом исследования угроз безопасности ПДн является информационная система Организации, обрабатывающая ПДн.

Целью построения данной модели угроз безопасности ПДн является получение полного перечня УБПДн, выявление среди них актуальных, которые могут быть реализованы в ИСПДн Организации, и могут привести к деструктивным действиям в отношении ПДн, обрабатываемых в информационных системах.

Целью построения Модели нарушителя информационной безопасности является определение возможностей потенциальных нарушителей с целью выработки технических мер по защите от них, в части криптографической защиты ПДн, обрабатываемых в ИСПДн Организации.

Моделирование моделей проводилось на основании действующих документов ФСБ и ФСТЭК России по защите ПДн.

4. Основные результаты

4.1. Характеристики ИСПДн

При проведении обследования ФГБОУ ВО «РГСУ» был определен перечень информационных систем, обрабатывающих персональные данные:

ИСПДн «Абилимпикс» в составе:

- «Автоматизированная информационная система чемпионатов по профессиональному мастерству среди инвалидов и лиц с ограниченными возможностями здоровья «Абилимпикс».

Характеристики ИСПДн «Абилимпикс» представлены в Таблице 1.

Таблица 1. Характеристики ИСПДн «Абилимпикс»

Характеристика	
Категория обрабатываемых персональных данных	Специальные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	менее 100 000
Структура информационной системы	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации
Режим обработки персональных данных	многопользовательская
Режим разграничения прав доступа пользователей информационной системы	с разграничением прав доступа
Наличие подключения к сетям связи общего пользования и /или сетям международного информационно обмена	имеется

В соответствии с требованиями к защите персональных данных при обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01 ноября 2012 г. № 1119), для ИСПДн «Абилимпикс» актуальны угрозы 2-го типа и информационная система обрабатывает специальные персональные данные менее, чем 100.000 субъектов, не являющихся работниками оператора **необходимо обеспечение 2-го уровня защищенности.**

4.2. Описание процесса моделирования угроз безопасности персональных данных

Анализ и моделирование УБПДн проведены для получения качественной и количественной оценки реальных угроз, актуальных для ПДн, обрабатываемых в ИСПДн ФГБОУ ВО «РГСУ».

При разработке модели угроз безопасности ПДн, обрабатываемых в ФГБОУ ВО «РГСУ», в качестве основополагающих, использовались нормативные документы ФСБ и ФСТЭК России, определяющие подходы к безопасности ПДн:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Приказ ФСБ России 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности»;
- Постановление Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости;
- Методические рекомендации по составлению Частной модели угроз безопасности персональных при их обработке в ИСПДн учреждений и организаций здравоохранения, социальной сферы, труда и занятости.

Построение модели угроз безопасности ПДн основывалось на классификации, анализе и оценки актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.

В рамках построения модели угроз безопасности ПДн все вероятные угрозы были разделены на две категории:

- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам;
- угрозы безопасности ПДн, реализуемые за счет несанкционированного доступа к ПДн с использованием штатного или специально разработанного программного обеспечения.

В ходе моделирования идентифицированы все возможные источники угроз, все возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, все идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

4.2.1. Классификация угроз безопасности ПДн за счёт утечки ПДн по техническим каналам

При обработке ПДн в ИСПДн «Абилимпикс» возможно возникновение УБПДн за счет реализации следующих каналов утечки информации по техническому каналу:

- угрозы утечки видовой (визуальной) информации;
- угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

4.2.1.1. Угрозы утечки видовой информации

Источником угроз утечки видовой (визуальной) информации являются физические лица, не имеющие доступа к ИСПДн «Абилимпикс», а также технические средства просмотра, внедренные в служебные помещения или скрытно используемые данными физическими лицами.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Угрозы утечки видовой (визуальной) информации реализуются за счет просмотра ПДн с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, входящих в состав ИСПДн «Абилимпикс».

4.2.1.2. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок

Источником угроз утечки информации по каналам ПЭМИН являются физические лица, не имеющие доступа к ИСПДн «Абилимпикс».

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническим средствами ИСПДн «Абилимпикс».

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн «Абилимпикс» в виде электрических информативных сигналов, ее обработка и передача по электрическим цепям техническими средствами ИСПДн «Абилимпикс» сопровождается побочными электромагнитными излучениями.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн, путем использования аппаратуры в составе радиоприемных устройств, предназначенной для восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн ("аппаратные закладки").

4.2.2. Угрозы несанкционированного доступа к информации, обрабатываемой в ИСПДн «Абилимпикс».

В ИСПДн «Абилимпикс» угрозы НСД с применением программных и аппаратно-программных средств, которые реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения, несанкционированного ознакомления), целостности (уничтожения, изменения), достоверности и доступности (блокирования) ПДн, включают в себя:

- угрозы доступа (проникновения) в операционную среду сервера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ);
- угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;
- угрозы внедрения вредоносных программ (программ математического воздействия);
- угрозы НСД, возникающие за счет непреднамеренных действий обслуживающего персонала системы.

Кроме того, возможны комбинированные угрозы, представляющие собой сочетание указанных угроз. Например, за счет внедрения вредоносных программ могут создаваться условия для НСД в операционную среду сервера, в том числе путем формирования нетрадиционных информационных каналов доступа.

Угрозы доступа (проникновения) в операционную среду ИСПДн «Абилимпикс» с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и аппаратно-программных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы, так как

количество вредоносных программ уже значительно превышает сотни тысяч. Для осуществления защиты информации достаточно знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования).

4.2.3. Общая характеристика уязвимостей ИСПДн «Абилимпикс»

Уязвимость ИСПДн «Абилимпикс» – недостаток или слабое место в системном, прикладном, программном и/или аппаратно-программном обеспечении системы, которое может быть использовано для реализации угрозы безопасности персональных данных.

Причиной возникновения уязвимостей являются:

- ошибки при проектировании и разработке программного и/или аппаратно-программного обеспечения;
- преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного и/или аппаратно-программного обеспечения;
- неправильные настройки программного и/или аппаратно-программного обеспечения, неправомерное изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и т.д.);
- сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств, внесение изменений в документацию и др.).

Различают следующие группы основных уязвимостей:

- уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
- уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

4.2.3.1. Уязвимости системного программного обеспечения

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем:

- в микропрограммах, в прошивках запоминающих устройств;
- в средствах ОС, предназначенных для управления локальными ресурсами ИСПДн «Абилимпикс» (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода/вывода, интерфейсом с пользователем и т.п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиков и т.п.), программах представления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.п.);
- в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
- фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

4.2.3.2. Уязвимости прикладного программного обеспечения

К прикладному программного обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – текстовые и графические редакторы, медиа-программы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т.п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа Delphi, Visual Basic), средства защиты информации общего пользования и т.п.

Уязвимости прикладного программного обеспечения могут представлять собой:

• функции и процедуры, относящие к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;

• функции, процедуры, изменение определенным образом параметров которых позволяет использовать их для проникновения в операционную среду ИСПДн «Абилимпикс», а также использования штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;

• фрагменты кода программ ("дыры", "закладки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;

• отсутствие необходимых средств защиты (аутентификации, проверка целостности, проверка форматов сообщений, блокирование несанкционировано модифицированных функций и т.п.);

• ошибки в программах (в объявлении переменных, функций и процедур, кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

4.2.4. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн «Абилимпикс»

Для ИСПДн «Абилимпикс» можно рассматривать следующие угрозы непосредственного доступа в операционную среду:

• угрозы, реализуемые в ходе загрузки ОС, направлены на перехват паролей или идентификаторов, модификацию ПО базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации получения НСД в операционную среду ИСПДн «Абилимпикс». Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации;

• угрозы, реализуемые после загрузки операционной системы, направлены на выполнение несанкционированного доступа к информации с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, а также с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);

• угрозы внедрения вредоносных программ. Реализация данных угроз определяется тем, какая из прикладных программ запускается пользователем или фактом запуска любой из прикладных программ.

4.3. Определение уровня исходной защищенности

Определение уровня исходной защищенности производилось в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их

обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России от 14 февраля 2008 г.

4.3.1. Определение уровня исходной защищенности ИСПДн «Абилимпикс»

Таблица 3. Показатели исходной защищенности ИСПДн «Абилимпикс»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности
1. По территориальному размещению	средний
2. По наличию соединения с сетями общего пользования	средний
3. По встроенным (легальным) операциям с записями баз персональных данных	низкий
4. По разграничению доступа к персональным данным	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	высокий
6. По уровню обобщения (обезличивания) ПДн	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	средний

Исходя из анализа предоставленных данных, уровень исходной защищенности данных ИСПДн может быть оценен как «средний», исходя из того, что более 70% характеристик соответствуют уровню «средний» или выше.

При составлении перечня актуальных угроз безопасности ПДн полученной оценке степени исходной защищенности ставится в соответствие числовой коэффициент: **Y1 = 5**

4.4. Определение вероятности реализации угроз в ИСПДн «Абилимпикс»

Под вероятностью реализации угрозы понимается, определяемый экспертным путем, показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн «Абилимпикс» в складывающихся условиях обстановки.

Числовой показатель (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2=2);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2=5);

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2=10).

4.5. Определение вероятности реализации угроз в ИСПДн «Абилимпикс» и перечня актуальных угроз безопасности

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Угрозы утечки по техническим каналам передачи/обработки данных					
По видовым каналам					
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	2	0,35	Средняя	Низкая	Неактуально
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	0,35	Низкая	Средняя	Неактуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором, ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Просмотр информации с помощью специальных электронных устройств внедренных в помещение, в котором ведется обработка персональных данных	0	0,25	Низкая	Низкая	Неактуально
Угрозы НСД по программно-аппаратному каналу					
Угроза доступа/перехвата/изменения HTTP cookies	5	0,5	Высокая	Высокая	Актуально
Угрозы, связанные с НСД к базовой системе ввода-вывода	5	0,5	Высокая	Средняя	Актуально
Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных	5	0,5	Высокая	Средняя	Актуально
Угрозы модификации настроек	5	0,5	Высокая	Средняя	Актуально
Угрозы внедрения вредоносного ПО	5	0,5	Высокая	Средняя	Актуально
Угрозы возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения	5	0,5	Высокая	Средняя	Актуально
Угрозы фишинга	5	0,5	Высокая	Высокая	Актуально
Угрозы несанкционированного доступа к виртуальным машинам, гипервизору.	5	0,5	Высокая	Высокая	Актуально
Угроза межсайтового скриптинга	10	1	Высокая	Высокая	Актуально
Угроза межсайтовой подделки запроса	10	1	Высокая	Средняя	Актуально
Угроза неправомерных действий в каналах связи	10	1	Высокая	Высокая	Актуально
Угроза несанкционированного восстановления удалённой защищаемой информации	10	1	Высокая	Высокая	Актуально
Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	10	1	Высокая	Высокая	Актуально
Угроза «форсированного веб-браузинга»	2	0,35	Высокая	Низкая	Актуально
Угроза «спама» веб-сервера	2	0,35	Высокая	Низкая	Актуально
Угроза несанкционированного изменения параметров	10	1	Высокая	Высокая	Актуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (К3)	Актуальность угрозы
настройки средств защиты информации					
Угроза несанкционированного воздействия на средство защиты информации	10	1	Высокая	Высокая	Актуально
«Отказ в обслуживании»	2	0,35	Высокая	Низкая	Актуально
Угроза изменения режимов работы аппаратных элементов	5	0,5	Высокая	Средняя	Неактуально
Угроза несанкционированного удаленного внелокального доступа	5	0,5	Высокая	Высокая	Неактуально
Угроза эксплуатации цифровой подписи программного кода	2	0,35	Средняя	Низкая	Неактуально
Несанкционированное отключение средств защиты	5	0,5	Высокая	Средняя	Неактуально
Угроза исследования механизмов работы программ	0	0,25	Низкая	Низкая	Неактуально
Угроза неправомерных действий в каналах связи	2	0,35	Низкая	Средняя	Неактуально
Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)					
Компьютерные вирусы	5	0,5	Высокая	Средняя	Актуально
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	0,25	Низкая	Низкая	Неактуально
Установка ПО, не связанного с исполнением служебных обязанностей	5	0,5	Средняя	Средняя	Актуально
Наличие аппаратных закладок в приобретаемых ПЭВМ	0	0,25	Низкая	Средняя	Неактуально
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	0	0,25	Низкая	Средняя	Актуально
Внедрение аппаратных закладок сотрудниками организации	2	0,35	Низкая	Средняя	Актуально
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	0	0,25	Низкая	Средняя	Актуально
Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера					
Угроза утраты носителей информации	5	0,5	Высокая	Средняя	Актуально
Непреднамеренная модификация (уничтожение)	5	0,5	Высокая	Средняя	Актуально

Наименование угрозы	Коэф. опред. вероятность наступления угрозы (Y2)	Коэффициент реализуемости угрозы (Y=(Y1+Y2)/20)	Возможность реализации угрозы	Опасность угрозы (КЗ)	Актуальность угрозы
информации сотрудниками					
Непреднамеренное отключение средств защиты	2	0,35	Средняя	Средняя	Актуально
Выход из строя аппаратно-программных средств	2	0,35	Высокая	Средняя	Актуально
Сбой системы электроснабжения	0	0,25	Низкая	Низкая	Неактуально
Стихийное бедствие	0	0,25	Средняя	Низкая	Неактуально
Угрозы преднамеренных действий внутренних нарушителей					
Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	2	0,35	Низкая	Средняя	Неактуально
Угроза несанкционированного копирования защищаемой информации	5	0,5	Высокая	Средняя	Актуально
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	0,5	Высокая	Средняя	Актуально
Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	0	0,25	Высокая	Средняя	Актуально
Угроза неправомерного ознакомления с защищаемой информацией	2	0,35	Средняя	Средняя	Актуально
Утечка атрибутов доступа	5	0,5	Высокий	Средняя	Актуально
Перехват за пределами контролируемой зоны	5	0,5	Высокий	Средняя	Актуально
Перехват в пределах контролируемой зоны внешними нарушителями	5	0,5	Высокая	Средняя	Неактуально
Перехват в пределах контролируемой зоны внутренними нарушителями	5	0,5	Высокая	Средняя	Неактуально

Актуальными угрозами безопасности ИСПДн «Абилимпикс» являются:

- Угроза доступа/перехвата/изменения HTTP cookies;
- Угрозы, связанные с НСД к базовой системе ввода-вывода;
- Угрозы, реализуемые после загрузки ОС, направленные на уничтожение, копирование, перемещение, искажение данных;
- Угрозы модификации настроек;
- Угрозы внедрения вредоносного ПО;
- Угроза возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения;
- Угрозы фишинга;
- Угрозы несанкционированного доступа к виртуальным машинам, гипервизору;
- Угроза межсайтового скриптинга;
- Угроза межсайтовой подделки запроса;
- Угроза неправомерных действий в каналах связи;

- Угроза несанкционированного восстановления удалённой защищаемой информации;
- Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL;
- Угроза «форсированного веб-браузинга»;
- Угроза «спама» веб-сервера;
- Угроза несанкционированного изменения параметров настройки средств защиты информации;
- «Отказ в обслуживании»;
- Компьютерные вирусы;
- Установка ПО, не связанного с исполнением служебных обязанностей;
- Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн;
- Внедрение аппаратных закладок сотрудниками организации;
- Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями);
- Угроза утраты носителей информации;
- Непреднамеренная модификация (уничтожение) информации сотрудниками;
- Непреднамеренное отключение средств защиты;
- Выход из строя аппаратно-программных средств;
- Угроза несанкционированного копирования защищаемой информации;
- Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке;
- Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;
- Угроза неправомерного ознакомления с защищаемой информацией;
- Утечка атрибутов доступа;
- Перехват за пределами контролируемой зоны.

5. Модель нарушителя безопасности персональных данных при их обработке в ИСПДн «Абилимпикс»

На основании назначения ИСПДн «Абилимпикс» к нарушителям информационной безопасности ИСПДн «Абилимпикс»следует отнести субъекты следующих категорий:

а. неустановленные внешние субъекты (физические лица);

б. преступные группы;

в. разработчики, производители, поставщики программных, технических и программно-технических средств;

г. лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

д. лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ;

е. пользователи информационной системы;

ж. администраторы информационной системы и администраторы безопасности;

Упомянутые выше потенциальные нарушители информационной безопасности ИСПДн, в большинстве своем не способны самостоятельно проводить лабораторные исследования криптосредств и/или средств, обеспечивающих их функционирование, а также иметь отношения к научно-исследовательским организациям, которые могут самостоятельно осуществлять анализ средств криптографической защиты информации и программно-технической среды их функционирования, а также разработку способов атак на них. В связи с

этим, подобные исследовательские организации могут являться нарушителями информационной безопасности ИСПДн «Абилимпикс» исключительно в случае их привлечения к этому со стороны нарушителей, перечисленных выше типов: а) – ж) путем организации сговора. При этом, поскольку такие научно-исследовательские организации, как правило, не могут рассматриваться как участники рынка, характерного для Организации, подобный сговор должен рассматриваться как совершаемый ими из корыстных побуждений. Вместе с тем, если учесть характер данных, которые обрабатываются, хранятся и передаются между объектами ИСПДн «Абилимпикс», наличие такого рода сговора между нарушителями информационной безопасности систем Организации и специализированными исследовательскими организациями представляется маловероятным. По той же причине представляется невозможным привлечение этих организаций для реализации атак на ИСПДн «Абилимпикс» физическими лицами (бывшими или действующими сотрудниками Организации)

Модель нарушителя информационной безопасности ИСПДн «Абилимпикс» строилась исходя из конкретных категорий субъектов, их квалификации и мотивации действий с учетом используемых технологий обработки информации. Перечень видов и категорий нарушителей безопасности ПДн, обрабатываемых в ИСПДн «Абилимпикс» приведен в Таблице 4:

Таблица 4. Виды и категории нарушителей безопасности ПДн

Вид нарушителя	**Категория нарушителя**
Внешние	1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону
Внутренние	1. Зарегистрированные пользователи ИСПДн «Абилимпикс» (пользователи, администраторы). 2. Незарегистрированные пользователи ИСПДн, но имеющие право доступа в контролируемую зону.

При построении модели нарушителя принимались следующие ограничения и предположения о характере действий нарушителей:

- несанкционированный доступ может быть следствием как случайных, так и преднамеренных действий;
- нарушитель, планируя атаки, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности;
- проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды функционирования криптосредств, не является целесообразным для нарушителей с учетом характера данных, обрабатываемых в ИСПДн «Абилимпикс».

5.1. Внешние нарушители

Внешний нарушитель не имеет права свободного доступа к системам и ресурсам ИСПДн «Абилимпикс», находящимся в пределах контролируемой зоны, и может осуществлять атаки только с территории, расположенной вне контролируемой зоны, через выходящие за пределы контролируемой зоны каналы связи, а также технические каналы утечки информации.

К данному виду нарушителей относится внешний нарушитель, не имеющий прав доступа в контролируемую зону.

5.1.1. Внешний нарушитель, не имеющий прав доступа в контролируемую зону

5.1.1.1. Описание нарушителей

Внешние нарушители данного вида характеризуются тем, что, как правило, не имеют возможности прямого доступа к элементам ИСПДн «Абилимпикс», но при этом не исключается возможность доступа к коммуникационным линиям и оборудованию ИСПДн

«Абилимпикс», расположенным вне контролируемой зоны. Среди данного вида нарушителей можно выделить:

- неустановленных внешних субъектов;
- преступные группы;
- разработчики, производители, поставщики программных, технических и программно-технических средств.

5.1.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Внешний нарушитель данного типа может иметь доступ к любому объему данных, распространяемому согласно установленному порядку и с помощью штатных средств системы по внешним каналам связи вне охраняемой зоны. Также он может располагать определенными фрагментами информации о топологии сети, об используемых коммуникационных протоколах и их сервисах, об особенностях используемого оборудования, системного, прикладного ПО и т.д. в объемах, доступных в свободной продаже.

Внешний нарушитель не должен (но гипотетически может) располагать именами зарегистрированных пользователей ИСПДн «Абилимпикс», может вести разведку имен и паролей зарегистрированных пользователей.

5.1.1.3. Предположения об имеющихся у нарушителя средствах атаки

Предполагается, что внешний нарушитель данного вида для реализации своих целей может обладать доступными в свободной продаже следующими техническими средствами и программным обеспечением:

- средствами вычислительной техники (аппаратными и программными) общего назначения;
- техническими и программными средствами, аналогичным средствам ИСПДн «Абилимпикс», включая соответствующие средства каналообразования, маршрутизации и т.д.;
- техническими и программными средствами защиты информации, включая СКЗИ, аналогичные используемым в ИСПДн «Абилимпикс»;
- специализированными техническими и программными средствами, предназначенными для перехвата информации в общедоступных каналах связи.

5.1.1.4. Описание каналов атак

Нарушители данного вида могут осуществлять атаки только из-за пределов контролируемой зоны через выходящие за пределы контролируемой зоны каналы связи, в том числе с использованием иных технических каналов утечки информации:

- проводить перехват и последующий анализ данных, циркулирующих по общедоступным каналам связи между отдельными элементами ИСПДн «Абилимпикс»;
- проводить попытки уничтожения, модификации и блокирования информации, передаваемой, обрабатываемой и хранимой в ИСПДн «Абилимпикс»;
- проводить попытки навязывания ложной информации;
- внедрять вредоносное ПО;
- проводить атаки с целью вызвать отказы в работе отдельных компонентов ИСПДн «Абилимпикс».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления. Нарушители данного вида не могут использовать для реализации атак штатные средства ИСПДн «Абилимпикс».

5.2. Внутренние нарушители

К внутренним нарушителям относятся лица, имеющие право постоянного или разового доступа к техническим средствам и информационным ресурсам ИСПДн «Абилимпикс»:

- зарегистрированные пользователи ИСПДн «Абилимпикс»;
- администраторы информационных систем и администраторы безопасности;
- лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора;

• лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ.

В связи с этим принимаются следующие ограничения и предположения о характере действий потенциальных внутренних нарушителей:

• работа по подбору кадров и специально проводимые организационно-технические мероприятия исключают возможность создания коалиций нарушителей, то есть объединения (заговоров) и направленных действий по преодолению подсистемы защиты двух и более нарушителей;

• несанкционированные действия нарушителей могут не иметь преднамеренного характера и быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала;

• легальный доступ посторонних лиц в помещения, где размещены компоненты ИСПДн «Абилимпикс», и к информационным ресурсам ИСПДн исключается принятыми организационными и/или техническими мерами по обеспечению порядка доступа в помещения, охране территории и организации пропускного режима на объектах, а также внедрением необходимых защитных мер и устройств в оборудование ИСПДн;

По возможным сценариям воздействия внутренние нарушители могут быть классифицированы как злоумышленники, то есть лица, которые целенаправленно стараются преодолеть систему защиты и нанести ущерб, и нарушители, которые совершают несанкционированные действия неумышленно, но эти действия также могут нанести ущерб и должны учитываться при построении системы защиты.

Возможности внутреннего нарушителя существенно зависят от действующих в пределах контролируемой зоны ограничительных факторов, реализации комплекса административных, режимных и организационно-технических мер, направленных на предотвращение и пресечение несанкционированных действий пользователей и администраторов системы, нарушения порядка допуска и контроля сторонних лиц внутри контролируемой зоны, предотвращение несанкционированного доступа пользователей к ресурсам ИСПДн «Абилимпикс», а также контроль за порядком обращения конфиденциальной информации.

5.2.1. Сотрудник внешней организации, не являющийся зарегистрированным пользователем ИСПДн «Абилимпикс», но имеющий право доступа в контролируемую зону

5.2.1.1. Описание нарушителей (субъектов атак)

Данный вид нарушителя характеризуются тем, что имеют возможность по доступу к элементам ИСПДн и их коммуникационным линиям. К внутренним нарушителям данного вида относятся лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных работ, имеющие доступ в помещения, где установлено оборудование ИСПДн «Абилимпикс».

5.2.1.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что нарушители данного типа дополнительно к информации, имеющейся у внешнего нарушителя и описанной в п. 5.1.1.2, могут иметь представление об организации работы пользователей, порядке и правилах создания, хранения и передачи информации.

5.2.1.3. Предположения об имеющихся у нарушителях средствах атак

Предполагается, что внутренний нарушитель данного вида дополнительно к средствам осуществления атак, описанных выше в пункт 5.1.1.3, может использовать серийно изготовляемое специальное оборудование и свободно распространяемое ПО, предназначенные для сканирования и копирования информационных ресурсов рабочих станций, изменения конфигураций рабочих станций, включая конфигурации средств защиты информации и/или внесения в систему вредоносного программного кода.

5.2.1.4. Описание каналов атак

Дополнительно к атакам, доступным нарушителю, описанному в п. 5.1.1.4, рассматриваемый тип нарушителя может осуществлять попытки несанкционированного доступа к ресурсам ИСПДн «Абилимпикс» с целью получения информации, ее подмены или уничтожения, включая обход существующих средств защиты информации, с использованием следующих атак:

- получения аутентификационной информации легальных пользователей посредством сканирования открытых портов на рабочих станциях и серверах;
- атак, основанных на переполнении буфера, генерируемых с использованием специализированных программных средств;
- внедрения вредоносного ПО;
- попыток временной или полной остановки работы посредством атак класса «отказ в обслуживании».

Доступным источником конфиденциальной информации для данного вида нарушителей могут быть отчуждаемые носители информации, выведенные установленным порядком из употребления.

5.2.2. Зарегистрированные пользователи ИСПДн «Абилимпикс»

Зарегистрированный пользователь ИСПДн «Абилимпикс» имеет санкционированный доступ к работе в системе с использованием штатных аппаратных и программных средств.

5.2.2.1. Описание нарушителей (субъектов атак)

Зарегистрированный пользователь, имеющий статус администратора и отвечающий за обеспечение безопасности, обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, в том числе и к средствам криптозащиты, обладает правами конфигурирования и административной настройки. Единственным исключением для таких пользователей может являться отсутствие доступа ко всему объекту ключевой информации, используемой в системе. Зарегистрированные пользователи такой категории относятся к числу привилегированных пользователей, назначаемых из числа особо доверенных лиц. Реализация необходимых организационно-технических мер, обеспечивающих выполнение требований по безопасности при приеме на работу данной категории работников, а также контроль за выполнением ими своих должностных обязанностей и соблюдением установленных правил и инструкций позволяет не рассматривать их в качестве потенциальных нарушителей.

Предполагается также, что пользователи, осуществляющие удаленный доступ к защищаемым ресурсам, по своим возможностям не превосходят возможностей локальных пользователей, имеющих доступ к штатным средствам системы, и поэтому они отдельно не рассматриваются.

5.2.2.2. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что зарегистрированный пользователь знает, по меньшей мере, одно легальное имя доступа.

Кроме того, зарегистрированный пользователь может располагать всей информацией о топологии и технических средствах обработки информации сети, полным объемом конфиденциальных данных, к которым данный пользователь имеет доступ, и любыми фрагментами неконфиденциальных (не защищаемых от доступа данного пользователя) данных, обладать всеми необходимыми атрибутами, обеспечивающими доступ (паролем).

Зарегистрированный пользователь знает специфику задач, решаемых в ИСПДн «Абилимпикс», и функциональные особенности работы системы, а также хранения, обработки и передачи информации.

5.2.2.3. Предположения об имеющихся у нарушителя средствах атак

Нарушители данного вида обладают возможностями использования доступных в свободной продаже технических и программных средств для:

- внесения ошибок и программных закладок в системное и прикладное ПО;

- внедрения вредоносных программ;
- хищения, уничтожения, модификации, блокирования информации и навязывания ложной информации.

5.2.2.4. Описание каналов атак

Зарегистрированный пользователь дополнительно имеет возможность прямого физического и прямого (не межсетевого) доступа к некоторому подмножеству ресурсов сети. Прямой доступ к ресурсам может быть использован для атак на технические средства обработки информации.

Нарушители данного вида для реализации атак могут использовать каналы связи, расположенные как внутри, так и вне контролируемой зоны.

5.3. Определение типов нарушителей

При определении типа нарушителя в рамках данного документа оценивались:

- степень информированности нарушителя;
- возможность нарушителя по использованию средств атаки.

При определении ограничений на степень информированности нарушителя рассматривались следующие сведения:

- содержание технической документации на технические и программные компоненты СФК;
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от НСД к информации организационно-техническими мерами;
- сведения о линиях связи, по которым передается защищаемая информация;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства и СФК;
- все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических криптосредств и СФК;
- сведения, получаемые в результате анализа любых сигналов от технических криптосредств и СФК, которые может перехватить нарушитель.

Таблица 5. Соответствие типа нарушителя и степени его информативности

Тип нарушителей	Степень информированности
Н1 – Н2	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК
Н3 – Н6	Могут располагать информацией обо всех сетях связи, работающих на едином ключе
Н5 – Н6	Располагают наряду с доступной в свободной продаже документацией на криптосредство и СФК исходными текстами прикладного программного обеспечения
Н6	Располагает всей документацией на криптосредство и СФК

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, рассматривались:

- аппаратные компоненты криптосредства и СФК;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение;
- штатные средства.

Таблица 6. Возможности нарушителей по использованию средств атак

Тип нарушителя	Аппаратные компоненты криптосредства и СФК	Штатные средства	Лабораторные исследования
H1	Располагают только доступными в свободной продаже аппаратными компонентами криптосредства и СФК	Могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны	
H2		Возможности по использованию штатных средств зависят от реализованных в информационной системе организационных мер	
H3	Дополнительные возможности по получению аппаратных компонент криптосредства и СФК зависят от реализованных в информационной системе организационных мер		
H4			Могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы
H5			
H6	Располагают любыми аппаратными компонентами криптосредства и СФК		

В соответствии с классификацией ФСБ России и с учетом сформулированных предположений об имеющихся у нарушителей возможностях нарушители ИСПДн «Абилимпикс» подразделяются на следующие категории и типы, которые представлены в Таблице 7:

Таблица 7. Виды нарушителей безопасности персональных данных, обрабатываемых в ИСПДн «Абилимпикс»

Вид нарушителя	Категория нарушителя		Тип нарушителя
	Категория I	Категория II	
Внешние	Внешний нарушитель, не имеющий прав доступа в контролируемую зону	-	H1
Внутренние		1 Зарегистрированные пользователи ИСПДн Организации (пользователи)	H2
		2 Незарегистрированные пользователи ИСПДн, но имеющие право доступа в Контролируемую зону	H2

При этом возможности нарушителя типа Hi+1 включают в себя возможности нарушителя Hi ($1 \leq i \leq 5$), а следовательно, при выборе необходимого уровня криптографической защиты ПДн следует рассматривать наивысший тип.

Таблица 8. Классификация ИСПДн Организации по уровням защиты от НСД к ПДн.

ИСПДн Организации	Тип нарушителя	Уровень защиты от НСД к ПДн
ИСПДн «Абилимпикс»	Н2	АК2

5.4. Уровень криптографической защиты

Возможности внешнего и внутреннего нарушителя безопасности ПДн при их обработке в ИСПДн «Абилимпикс» соответствуют возможностям нарушителя типа Н1 и Н2 - соответственно, согласно классификации нарушителей, приведенной в приказе ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровня защищенности», и «Методических рекомендациях по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» утвержденные руководством 8 Центра ФСБ России от 31 марта 2015 № 149/7/2/6-432, криптографические средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Абилимпикс», должны обеспечивать криптографическую защиту по уровню не ниже уровня КС1.

5.5. Выводы

На основании проведенного анализа возможных угроз безопасности информации, в информационных системах персональных данных можно сделать следующие выводы:

1. Атаки внешнего нарушителя, направленные на каналы связи, посредством перехвата информации и последующего ее анализа, уничтожения, модификации и блокирования информации с использованием, в том числе, уязвимостей программной среды, а также утечка информации по техническим каналам подлежат нейтрализации организационными и техническими мероприятиями.

2. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

3. Ввиду исключительной роли в ИСПДн «Абилимпикс»лиц типа Н2, в число этих лиц должны включаться только доверенные лица, к которым применен комплекс особых организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

4. Лица типа Н2 относятся к вероятным нарушителям. Среди лиц типа Н2 наиболее опасными вероятными нарушителями являются пользователи ИСПДн и администраторы информационных систем, а также администраторы безопасности.

На основании построенной модели нарушителя, в частности, описания возможностей нарушителей и постановления Правительства от 01.11.2012 №1119 можно сделать вывод, что для ИСПДн «Абилимпикс» актуальны угрозы 3го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Представленная Модель угроз с описанием вероятного нарушителя для ИСПДн должна использоваться при формировании обоснованных требований безопасности информации и при проектировании СЗПДн ИСПДн. Средства защиты информации, используемые для защиты ПДн, обрабатываемых в ИСПДн «Абилимпикс», должны иметь сертификаты соответствия по требованиям информационной безопасности соответствующего класса.

Приложение № 3 к приказу
от «16» марта 2020 г.
№ 355

Федеральное государственное бюджетное образовательное учреждение высшего образования

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Кадры»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1 Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Кадры»:
- «1С: Управление образовательным процессом»;
- «1С: Зарплаты и кадры государственного учреждения 3.0»;
- «1С: Бухгалтерия государственного учреждения 2.0»;
- «1С: Зарплаты и кадры бюджетного учреждения 1.0»;
- «1С: Бухгалтерия государственного учреждения 1.0»;
- «1С: Розница»;
- «1С: Документооборот»;
- «Система дистанционного обучения»;
- «Веб-сайт»;
- Корпоративная почта;
- Корпоративный портал;
- «1С: Государственные муниципальные закупки»;
- «1С: Планово-финансовое управление»

Исходные данные для присвоения уровня защищенности ИСПДн «Кадры» РГСУ, представленные в Таблице 1

Таблица 1 - Исходные данные ИСПДн «Кадры»

Категория обрабатываемых ПДн	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000

Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить **4 уровень защищенности ПДн** при их обработке в ИСПДн «Кадры».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Обучающиеся»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Обучающиеся»:
- «1С: Управление образовательным процессом»;
- «1С: Зарплаты и кадры государственного учреждения 3.0»;
- «1С: Бухгалтерия государственного учреждения 2.0»;
- «1С: Зарплаты и кадры бюджетного учреждения 1.0»;
- «1С: Бухгалтерия государственного учреждения 1.0»;
- «1С: Библиотека»;
- «1С: Документооборот»;
- «Система дистанционного обучения»;
- «Портфолио»
- «Веб–сайт»;
- «1С: Конвертер «Московский социальный регистр»
- Корпоративный портал;

Исходные данные для присвоения уровня защищенности ИСПДн «Обучающиеся» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «Обучающиеся»

Категория обрабатываемых ПДн	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Более 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа

Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 1 ноября 2012 г. №1119

РЕШИЛА:

установить **3 уровень защищенности** ПДн при их обработке в ИСПДн «Обучающиеся».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Абитуриенты»

_____ № _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1 Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Абитуриенты»:
- «1С: Документооборот»;
- «Веб-сайт»;

Исходные данные для присвоения уровня защищенности ИСПДн «Абитуриенты» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «Абитуриенты»

Категория обрабатываемых ПДн	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Более 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить **3 уровень защищенности** ПДн при их обработке в ИСПДн «Абитуриенты».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Контрагенты»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Контрагенты»:
- «1С: Отель»;
- «1С: Розница»;
- «1С: Документооборот»;
- «Веб-сайт»;
- «Корпоративная почта».

Исходные данные для присвоения уровня защищенности ИСПДн «Контрагенты» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «Контрагенты»

Категория обрабатываемых ПДн	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации

Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить **4 уровень защищенности** ПДн при их обработке в ИСПДн «Контрагенты».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Медицина»

_____ **№ _____**

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ Руководитель IT

Члены рабочей группы для организации и проведения работ Участник № 1
Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Медицина»:
- «1С: Документооборот»;
- Корпоративная почта;
- МИС «МЕДИАЛОГ»;
- МИС «Инфоклиника».

Исходные данные для присвоения уровня защищенности ИСПДн «Медицина» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «Медицина»

Категория обрабатываемых ПДн	Специальные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить **3 уровень защищенности** ПДн при их обработке в ИСПДн «Медицина».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «СКУД»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ — Руководитель IT

Члены рабочей группы для организации и проведения работ — Участник № 1
Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «СКУД»:

- ИС «PERCo».

Исходные данные для присвоения уровня защищенности ИСПДн «СКУД» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «СКУД»

Категория обрабатываемых ПДн	Биометрические персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	Без подключения
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119

РЕШИЛА:

установить **3 уровень защищенности** ПДн при их обработке в ИСПДн «СКУД».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Отдых и проживание»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ — Руководитель IT

Члены рабочей группы для организации и проведения работ — Участник № 1, Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Отдых и проживание»:

- «1С: Отель»;
- «1С: Фитнес»;
- Веб-сайт;
- Корпоративная почта;
- Корпоративный портал.

Исходные данные для присвоения уровня защищенности ИСПДн «Отдых и проживание» РГСУ, представленные в Таблице 16

Таблица 1 - Исходные данные ИСПДн «Отдых и проживание»

Категория обрабатываемых ПДн	Иные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000
Структура информационной системы	Корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	Без подключения
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 3, не связанные с наличием НДВ в системном и прикладном ПО

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119.

РЕШИЛА:

установить **4 уровень защищенности** ПДн при их обработке в ИСПДн «Отдых и проживание».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»
(РГСУ)

Акт определения уровня защищенности ПДн в ИСПДн «Абилимпикс»

_____ **№** _____

Рабочая группа в составе:

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1 Участник № 2

Комиссией был определен перечень информационных систем, обрабатывающих персональные данные в ИСПДн «Абилимпикс»:

- Автоматизированная информационная система чемпионатов по профессиональному мастерству среди инвалидов и лиц с ограниченными возможностями здоровья «Абилимпикс».

Исходные данные для присвоения уровня защищенности ИСПДн «Абилимпикс» РГСУ, представленные в Таблице 1:

Таблица 1 - Исходные данные ИСПДн «Абилимпикс»

Категория обрабатываемых ПДн	Специальные персональные данные
Состав обрабатываемых ПДн	В ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками оператора
Количество субъектов ПДн	Менее 100 000
Структура информационной системы	Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государства в целом.
Режим обработки персональных данных	Многопользовательский
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением доступа
Наличие подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена	имеется
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации
Тип актуальных угроз	Актуальны угрозы типа 2, связанные с наличием недокументированных возможностей в прикладном программном обеспечении

Рабочая группа на основании анализа исходных данных информационной системы и в соответствии с требованием к защите ПДн при их обработке в ИСПДн, руководствуясь постановлением Правительства РФ от 01 ноября 2012 г. № 1119.

РЕШИЛА:

установить **2 уровень защищенности ПДн** при их обработке в ИСПДн «Абилимпикс».

Руководитель рабочей группы для организации и проведения работ	Руководитель IT
Члены рабочей группы для организации и проведения работ	Участник № 1
	Участник № 2

Приложение № 4 к приказу
от «16» марта 2020 г.
№ 555

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «РГСУ»)

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2020 г.

1. Общие положения

1.1. Положение о порядке организации и проведения работ по защите персональных данных в ФГБОУ ВО «РГСУ» (далее – «Положение») устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных (далее – «ПДн») при их обработке в ФГБОУ ВО «РГСУ» (далее – «Организация»).

1.2. Настоящее Положение разработано в соответствии с законодательством РФ, в том числе в соответствии с:

– Федеральным законом от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «Федеральный закон № 152-ФЗ»);

– Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Действие настоящего документа распространяется на всех работников ФГБОУ ВО «РГСУ», выполняющих обработку персональных данных в ИСПДн, и на администраторов ИСПДн.

1.4. Работники Организации руководствуются нормами настоящего Положения, документами, руководящими и нормативными документами ФСТЭК РФ и регламентирующими документами, разработанными и утвержденными в ФГБОУ ВО «РГСУ» в целях защиты информации и персональных данных.

2. Основные понятия

2.1. **Автоматизированная обработка персональных данных** – обработка ПДн с помощью средств вычислительной техники (далее – «СВТ»).

2.2. **Аутентификация** – процедура проверки принадлежности субъекту доступа предъявленного им идентификатора.

2.3. **Блокирование персональных данных** – временное прекращение обработки ПДн (за исключением случаев, при которых обработка необходима для уточнения ПДн).

2.4. **Вредоносное программное обеспечение** – программное обеспечение заведомо созданное для воздействия на информацию или активы информационной системы, и (или) получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, использования ресурсов ЭВМ; причинения вреда (нанесения ущерба) владельцу информации, и (или) владельцу ЭВМ, и (или) владельцу сети ЭВМ;

2.5. **Допуск** – это право (возможность) субъекта доступа на получение информации и её использование.

2.6. **Доступ к информации** – возможность получения информации и ее использования.

2.7. **Доступность** – состояние информационной системы, при которой существует возможность ознакомления (работы) с информацией, содержащейся внутри информационной системы.

2.8. **Идентификация** – процедура присвоение субъектам и объектам идентификатора и сравнение идентификатора с перечнем присвоенных идентификаторов.

2.9. **Информационная система персональных данных** (далее – «ИСПДн») – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

2.10. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

2.11. **Контролируемая зона** – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей организации, а также транспортных средств.

2.12. **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2.13. **Криптосредство** – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (далее – «СКЗИ»).

2.14. **Ответственный за организацию обработки персональных данных** – должностное лицо организации, осуществляемое деятельность по обеспечению информационной безопасности (далее – «ИБ»).

2.15. **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

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

2.17. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн).

2.18. **Правила разграничения доступа** – это совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

2.19. **Предоставление персональных данных** – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

2.20. **Распространение персональных данных** – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

2.21. **Субъект доступа** – это лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.22. **Субъект персональных данных** (далее – «Субъект ПДн») – физическое лицо, к которому относятся ПДн.

2.23. **Угроза безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в ИСПДн.

2.24. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

2.25. **Управление доступом** – механизм безопасности, который управляет процессом взаимодействия пользователей с информационными системами и ресурсами, а также информационными системами между собой.

2.26. **Уровень защищенности персональных данных** – комплексный показатель, устанавливаемый Правительством Российской Федерации с учетом объема и содержания обрабатываемых ПДн и актуальности угроз безопасности ПДн, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн.

2.27. **Целостность** – состояние информационной системы, при котором информация не может быть случайно или злонамеренно изменена, или уничтожена.

3. Организация обеспечения безопасности персональных данных

3.1. Безопасность ПДн достигается путем принятия необходимых правовых, организационных и технических мер для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в их отношении.

3.2. Для обеспечения безопасности ПДн приказом организации назначаются ответственный за организацию обработки персональных данных, администратор информационной безопасности ИСПДн и администратор ИСПДн.

3.3. **Ответственный за организацию обработки персональных данных обязан:**

- осуществлять внутренний контроль за соблюдением работниками организации установленных требований по обеспечению безопасности ПДн;
- организовывать проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- осуществлять контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- периодически инициировать процедуры определения угроз безопасности ПДн при их обработке в ИСПДн;
- организовывать и контролировать процедуры обнаружения фактов несанкционированного доступа к ПДн; фактов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- организовывать и контролировать процедуры принятия мер по предотвращению несанкционированного доступа к ПДн; инцидентов, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

3.4. **Администратор информационной безопасности ПДн обязан:**

- Осуществлять установку, настройку и сопровождение технических средств защиты.
- Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
- Участвовать в приемке новых программных средств.
- Обеспечить доступ к защищаемой информации Пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
- Уточнять в установленном порядке обязанности Пользователей ИСПДн по обработке объектов защиты.
- Вести контроль над процессом осуществления резервного копирования объектов защиты.
- Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
- Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- Контролировать физическую сохранность средств и оборудования ИСПДн.
- Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.
- Контролировать исполнение пользователями парольной политики.
- Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
- Не допускать к работе на элементах ИСПДн посторонних лиц.
- Осуществлять периодические контрольные проверки носителей ПДн, рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
- Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях

установленных требований по защите информации.

- В случае отказа работоспособности технических средств и программного обеспечения средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3.5. **Администратор ИСПДн обязан:**

- Поддерживать текущий порядок обеспечения безопасности ПДн;
- Организовывать доведение до сведения работников организации положений законодательства РФ и локальных нормативных документов по обеспечению безопасности ПДн;
- Определять перечень работников организации, которым доступ к ПДн необходим для выполнения служебных обязанностей;
- Участвовать в реализации планов и программ поддержки осведомленности (обучения) в области обеспечения ИБ;
- В случае отказа работоспособности технических средств и программного обеспечения ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;
- Принимать меры по реагированию, в случае возникновения непредвиденных и аварийных ситуаций, с целью ликвидации их последствий;

3.6. Необходимые технические меры для обеспечения безопасности ПДн реализуются в рамках системы защиты персональных данных (далее – СЗПДн).

3.7. СЗПДн обеспечивает защиту информации, содержащей ПДн, обрабатываемой с применением СВТ, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

3.8. Мероприятия по обеспечению безопасности ПДн, реализуемые в рамках СЗПДн, включают:

- определение уровня защищенности ИСПДн;
- создание моделей угроз и нарушителя для каждой ИСПДн;
- применение организационных и технических мер по обеспечению безопасности ПДн для поддержания установленного уровня защищенности ПДн и нейтрализации актуальных угроз безопасности ПДн;
- определение во внутренних нормативных документах порядка применения мер защиты, применяемых для обеспечения безопасности ПДн;
- ознакомление работников организации, непосредственно осуществляющих обработку ПДн, с требованиями законодательных и нормативных актов, локальных нормативных документов, устанавливающих порядок обеспечения безопасности ПДн;
- организацию внутреннего контроля и (или) аудита соответствия порядка обеспечения безопасности ПДн требованиям законодательных и нормативных актов, локальных нормативных документов;
- организацию обучения, инструктажей и повышения осведомленности работников, осуществляющих обработку ПДн, по вопросам обеспечения безопасности ПДн;
- совершенствование СЗПДн в соответствии с изменяемыми внутренними и внешними условиями и факторами, в том числе изменениями требований законодательства РФ.

4. Требования к системе защиты персональных данных

4.1. Требования к СЗПДн устанавливаются исходя из уровня защищенности ПДн и состава актуальных угроз безопасности ПДн.

4.2. Определение уровней защищенности ИСПДн производится в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.3. Определение угроз безопасности ПДн производится в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в

информационных системах персональных данных» (утверждено заместителем директора ФСТЭК России от 14.02.2008) на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России от 15.02.2008).

5. Описание системы защиты персональных данных

5.1. В число мер по обеспечению безопасности ПДн, реализованных в организации, входят:

- определение порядка доступа в помещения, в которых осуществляется обработки ПДн;
- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн (в том числе серверное помещение), а также хранятся носители информации;
- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным активам, информационной системе и связанным с ее использованием работам, документам только для выполнения функциональных обязанностей;
- установление правил доступа пользователей и обслуживающего персонала к информационным активам, программным средствам обработки (передачи) и защиты информации на основе принципа минимально необходимых полномочий для выполнения своих функциональных обязанностей и поставленными перед ним задачами в объеме, необходимом для их исполнения;
- учет и контроль лиц, допущенных к работе с ПДн;
- регистрация и учет действий пользователей с ПДн, контроль несанкционированного доступа к ПДн;
- размещение технических средства обработки графической, видео и буквенно-цифровой информации, содержащей ПДн, таким образом, чтобы исключить возможность просмотра посторонними лицами текстовой и графической, видовой информации, содержащей ПДн;
- использование СВТ, удовлетворяющих требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видео-дисплейным терминалам средств вычислительной техники;
- учет и хранение съемных носителей, содержащих ПДн, и их обращение, исключающее хищение, подмену и уничтожение;
- предотвращение внедрения в ИСПДн вредоносного программного обеспечения;
- применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

организация контроля за принимаемыми мерами по обеспечению безопасности ПДн и установленного уровня защищенности ПДн.

5.2. Для реализации указанных мер в составе СЗПДн реализованы следующие функциональные подсистемы:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- обеспечение целостности информационной системы и ПДн;
- обеспечение доступности ПДн;
- регистрация событий безопасности;
- антивирусная защита;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

5.3. Технические средства защиты информации, используемые для нейтрализации актуальных угроз безопасности ПДн, применяемые организацией, проходят в установленном порядке процедуру оценки соответствия.

5.3.1. Для выбора и реализации мер защиты ПДн организацией могут привлекаться на договорной основе сторонние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

6. Контроль выполнения требований

6.1. Контроль и надзор за выполнением требований по обработке ПДн осуществляется уполномоченным органом по защите прав субъектов ПДн (Роскомнадзор).

6.2. Федеральные органы исполнительной власти (ФСБ России и ФСТЭК России) могут осуществлять контроль за выполнением организационных и технических мер по обеспечению безопасности ПДн без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

6.3. Для проведения аудита соответствия порядка обеспечения безопасности ПДн требованиям законодательства РФ могут привлекаться внешние организации, имеющие оформленную в установленном порядке лицензию на соответствующий вид деятельности в области защиты информации.

7. Ответственность

7.1. Обязанности по контролю выполнения положений настоящего Положения возлагаются на Ответственного за организацию обработки персональных данных.

7.2. Ответственность за общий контроль реализации мероприятий по обеспечению безопасности ПДн несет Администратор безопасности ИСПДн.

ЛИСТ СОГЛАСОВАНИЯ

Должность	Роль	ФИО	Дата	Подпись
	Ответственный за организацию обработки ПДн			
	Администратор ИБ			
	Администратор ИСПДн			

Приложение № 5 к приказу
от «16» марта 2020 г.
№ 355

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «РГСУ»)

ПОЛОЖЕНИЕ О РАЗГРАНИЧЕНИИ ПРАВ ДОСТУПА К ОБРАБАТЫВАЕМЫМ ПЕРСОНАЛЬНЫМ ДАННЫМ В ИСПДН

Москва, 2020 г.

1. Общие положения

1.1. В данном документе представлен список лиц, ответственных за обработку персональных данных в информационной системе персональных данных (далее - «ИСПДн»), а также их уровень прав доступа к обрабатываемым персональным данным.

1.2. Список лиц, ответственных за обработку персональных данных в ИСПДн, утверждается приказом РГСУ.

1.3. Уровень прав доступа для ИСПДн и представлен в Таблице №1:

Таблица № 1

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники Организации
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	
Пользователи ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ПДн.	- сбор - систематизация - накопление - использование - уточнение	

Приложение № 6 к приказу
от «16» марта 2020 г.
№ 355

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ»)
(ФГБОУ ВО РГСУ)

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В УНИВЕРСИТЕТЕ

Москва, 2020 г.

1. Перечень персональных данных, обрабатываемых ФГБОУ ВО «РГСУ»

В Таблице 1 представлен перечень персональных данных (далее – «ПДн»), обрабатываемых в ФГБОУ ВО «РГСУ», с указанием категорий субъектов ПДн.

Таблица 1

№	Категория субъектов ПДн	Группа ПДн
1	Работники РГСУ	фамилия, имя, отчество
		тип, серия, номер документа, удостоверяющего личность
		дата выдачи документа, удостоверяющего личность
		год, месяц, дата, место рождения
		адрес регистрации по месту жительства и/или по месту регистрации
		контактная информация, в том числе номер контактного телефона и адрес электронной почты
		идентификационный номер налогоплательщика
		номер страхового свидетельства государственного пенсионного страхования
		доходы
		должность
		фотография
		образование
		профессия
		табельный номер
		банковские реквизиты
		номер профсоюзного билета
		статус воинского учета, отношение к воинской обязанности, категория годности к военной службе, районный военный комиссариат, категория запаса, состав (профиль), полное кодовое обозначение военной учетной специальности, сведения о воинском учете
		семейное положение
		трудовой стаж
		сведения о пребывании за границей
		данные о социальных льготах
		данные полиса ОМС
		сведения об оказанных услугах
		гражданство
		данные разрешения на временное проживание
		тарифная ставка/оклад
		сведения об аттестации и повышении квалификации
		сведения об отчислениях в ФНС, ПФР и ФСС.
2	Члены семей работников РГСУ	фамилия, имя, отчество
		степень родства
		год, месяц, дата рождения.
3	Соискатели вакансий	фамилия, имя, отчество
		дата и место рождения

		паспортные данные
		адрес по прописке
		фактический адрес
		контактные данные
		семейное положение
		состав семьи
		сведения об образовании
		трудовой опыт.
4	Обучающиеся	фамилия. имя, отчество
		тип, серия, номер документа, удостоверяющего личность
		дата выдачи документа, удостоверяющего личность, информация о выдавшем его органе
		год, месяц, дата и место рождения
		адрес регистрации по месту жительства и/или по месту пребывания
		номер контактного телефона
		адрес электронной почты
		фотография
		образование
		профессия
		табельный номер
		идентификационный номер налогоплательщика
		банковские реквизиты
		номер профсоюзного билета
		статус воинского учета
		отношение к воинской обязанности
		категория годности к военной службы
		районный военный комиссариат
		категория запаса
		воинское звание, состав (профиль)
		полное кодовое обозначение военной учетной специальности
		номер страхового свидетельства государственного пенсионного страхования
		состояние здоровья
		социальное положение
		данные полиса ОМС
		сведения об оказанных услугах
		семейное положение.
5	Абитуриенты	фамилия, имя, отчество
		факультет/институт/филиал (кафедра)
		группа
		сведения об ученых степенях и званиях
		сведения о результатах вступительных испытаний
		анкетные и биографические данные
		сведения об образовании
		сведения о составе семьи
		паспортные данные
		сведения о воинском учете
		специальность (аспирантов, обучающихся)
		занимаемая должность (аспирантов. обучающихся)
		адрес по месту фактического проживания
		номер контактного телефона
		содержание договора на обучение
		данные из личного дела (приказы)
		перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин

		успеваемость, в том числе результаты промежуточной и итоговой аттестации
		сведения о выплачиваемой стипендии, материальной помощи
		данные о публикациях и участии в грантах (конкурсах)
		данные о профессии
		сведения о владении иностранными языками
		данные о наградах и поощрениях (олимпиадах)
		фотографическое изображение (содержащееся в личном деле, студенческом билете,
		пропуске, зачетной книжке обучающегося)
		банковские реквизиты обучающегося
		сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки)
		сведения по отпускам (академический)
		социальные льготы
		место и дата регистрации (вид на жительство, регистрация миграционной карты)
		адрес электронной почты
		сведения о договорах
		страховое свидетельство государственного пенсионного страхования
		сведения о состоянии здоровья
		иные сведения, с которыми абитуриент и обучающийся считает нужным ознакомить Организацию, либо дополнительная информация необходимая Организации.
6	**Контрагенты и работники контрагентов**	фамилия, имя, отчество
		должность
		контактная информация
		сведения о месте жительства
		паспортные данные
		ИНН
		реквизиты лицевого счета в банке
		сведения о доходах.
7	**Пациенты Поликлиники РГСУ**	фамилия имя отчество
		паспортные данные и сведения о документе, удостоверяющем личность
		контактная информация
		дата и место рождения
		пол
		место жительства
		данные миграционной карты
		инвалидность
		семейное положение
		диагноз с места отбора
		диагноз санатория
		жалобы больного
		история настоящего заболевания
		стационарное лечение
		санаторно-курортное лечение
		перенесенные заболевания
		наследственность
		объективные данные (рост, масса тела, телосложение, кожные покровы и т.д.)
		состояние здоровья
		предварительный диагноз
		назначение врача

		итоги лечения
		сведения о регистрации
		данные разрешения на временное проживание
		ИНН
		номер страхового свидетельства государственного пенсионного страхования
		сведения о детях и родственниках
		иные сведения, предусмотренные трудовым законодательством и законодательством об организации предоставления медицинских услуг
8	**Пользователи иных услуг РГСУ**	анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.)
		паспортные данные
		адрес регистрации
		адрес фактического проживания
		номер контактного телефона
		адрес электронной почты
		данные о месте работы (при бронировании командируемых юридических лиц и ИП)
		номер банковской карты (в случае оплаты услуг таковой)

2. Цели обработки персональных данных

Цели обработки ПДн определены Организацией на основании требований:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона от 03.11.2006 № 174-ФЗ «Об автономных учреждениях»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Устава ФГБОУ ВО «РГСУ».