

УТВЕРЖДАЮ

Директор ГБУ СО ЯО

Дом социального
обслуживания «Забота»



М.В. Филиппова

2026 г.

ЧАСТНАЯ МОДЕЛЬ АКТУАЛЬНЫХ УГРОЗ И ВЕРОЯТНОГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

в государственном бюджетном учреждении социального обслуживания
Ярославской области Дом социального обслуживания «Забота»

1. Термины и определения

В настоящем документе используются следующие термины и определения:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся 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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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 в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно

внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

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

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.

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.

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 ее функционирования.

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

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

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.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц

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.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности ПДн.

2. Условные обозначения и сокращения

АРМ – автоматизированное рабочее место;

ВТСС – вспомогательные технические средства и системы;

ИСПДн – информационная система персональных данных;

КЗ – контролируемая зона;

НДВ – недеklarированные возможности;

НСД – несанкционированный доступ;

ОБПДн – обеспечение безопасности персональных данных;

ОС – операционная система;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;
 ПЭМИН – побочные электромагнитные излучения и наводки;
 СВТ – средство вычислительной техники;
 СЗИ – средство защиты информации;
 СЭУПИ – специальные электронные устройства перехвата информации;
 УБПДн – угрозы безопасности персональных данных.

3. Общие положения.

3.1. Частная модель актуальных угроз ГБУ СО ЯО Дом социального обслуживания «Забота» (далее Оператор) разработана в соответствии с нормативными документами в сфере защиты персональных данных:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная 15.02.2008 ФСТЭК России;
- Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (включая "Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости"), утвержденные Министерством здравоохранения и социального развития РФ 23.12.2009 г.).

3.2. Частная модель угроз содержит описание возможных угроз безопасности персональных данных и расчет актуальных угроз для ИСПДн Оператора.

3.3. Частная модель угроз направлена на определение возможных каналов утечки, путем анализа защищенности ИСПДн Оператора.

3.4 Под угрозами безопасности ПДн при их обработке в ИСПДн понимается 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.

3.5 В соответствии со статьей 19 Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных», ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

3.6 Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

4. Описание информационных систем персональных данных

4.1. В Учреждении существуют следующие типы ИСПДн:

1. ИСПДн ведения бухгалтерского учета, расчета заработной платы, кадровой деятельности Учреждения.

Информационная система представляет собой автоматизированную систему «Смета», включающую в себя кадровый учет, расчет зарплаты, бухгалтерский учет.

2. ИСПДн ведения учета получателей социальных услуг: Vipnet client и "Единый социальный регистр населения Ярославской области".

3. ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.

Состав ИСПДн и обрабатываемых в них персональных данных приведен в Приложении №1 к настоящему документу.

4.2. Информационные системы развернуты на компьютерах, которые имеют подключения к локальной сети и выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office». Операционная система – «Windows 7», «Windows 10», «Windows XP».

4.3. В качестве объекта информатизации предприятия выступают:

1. Автономные автоматизированные рабочие места (АРМ).

2. Локальные вычислительные сети.

4.4. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации. ИСПДн предполагают как распределенную (на АРМ), так и централизованную (на выделенных файловых серверах сети) обработку и хранение ПДн. Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных сотрудников Учреждения, как в электронном,

так и в бумажном виде.

4.5. Контролируемой зоной (КЗ) ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн.

4.6. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

5. Определение актуальных угроз безопасности персональных данных в ИСПДн

5.1. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников предприятия в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн. Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

5.2. Угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

- по видам возможных источников угроз;
- по типу ИСПДн, на которые направлена реализация угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по способам реализации угроз;
- по используемой уязвимости;
- по объекту воздействия.

5.3. Актуальность угрозы определяется следующими параметрами:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

5.4. Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

Характеристики ИСПДн

	Параметр	Значение	Уровень защищенности
--	----------	----------	----------------------

1	Территориальное размещение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Наличие соединений с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Встроенные (легальные) операции с записями баз персональных данных	запись, удаление, сортировка	средний
4	Разграничение доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Наличие соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Уровень обобщения (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	средний
7	Объем ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, не предоставляющие никакой информации	высокий

Значению уровня защищенности «Высокий» соответствуют 2 характеристики, значению уровня «Средний» - 5 характеристики, значению уровня «Низкий» - 0 характеристик. Таким образом, числовой коэффициент исходной защищенности ИСПДн Оператора соответствует значению 5 (средняя).

5.5. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

• высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2 , а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

5.6. Используя значения приведенных выше показателей Y_1 и Y_2 , вычисляется коэффициент реализуемости угрозы Y , определяемый соотношением $Y = (Y_1 + Y_2) / 20$.

В зависимости от своего значения этот коэффициент принимает значения:

$0 < Y < 0,3$ – реализуемость угрозы признается низкой;

$0,3 < Y < 0,6$ – реализуемость угрозы признается средней;

$0,6 < Y < 0,8$ – реализуемость угрозы признается высокой;

$Y > 0,8$ – реализуемость угрозы признается очень высокой.

Далее дается оценка опасности каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации.

5.7. Оценка опасности каждой угрозы имеет три значения:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

5.8. После просчета всех показателей производится оценка актуальности каждой угрозы безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице.

Реализуемость угрозы	Показатель опасности угрозы		
	низкий	средний	высокий
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

5.9. На основании положений модели угроз, модели нарушителя, данных об исходной защищенности ИСПДн (Y_1), коэффициенте реализуемости угрозы (Y), вероятности ее реализации (Y_2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы безопасности ПДн, обрабатываемых в ИСПДн.

6. Модель вероятного нарушителя безопасности персональных данных

6.1. По наличию права постоянного или разового доступа в ИСПДн нарушители подразделяются на два типа:

- нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена – внешние нарушители;
- нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн – внутренние нарушители.

6.2. Внешними нарушителями могут быть:

- представители криминальных структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

6.3. Внешний нарушитель имеет следующие возможности:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

6.4. Внутренний нарушитель подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К первой группе относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений учреждения, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;
- изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съём информации, используя непосредственное подключение к техническим средствам обработки информации.

2. Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места.

К этой категории относятся сотрудники учреждения, имеющие право доступа к

локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
- располагает ПДн, к которым имеет доступ.

3. К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети учреждения.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;
- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

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

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
- имеет доступ ко всем техническим средствам сегмента ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

5. К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о ТС и конфигурации ИСПДн - имеет доступ ко всем ТС ИСПДн и данным;
- обладает правами конфигурирования и административной настройки ТС ИСПДн.

6. К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности учреждения, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7. К седьмой группе относятся лица из числа программистов - разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

8. К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

Категории нарушителей

№	Описание	Нарушитель может	Возможный нарушитель
1	Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.	– иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; – располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; – располагать именами и вести выявление паролей зарегистрированных пользователей; – изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.	Сотрудники, не участвующие в обработке ПДн

2	Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.	– обладает всеми возможностями лиц первой категории; – знает по меньшей мере одно легальное имя доступа; – обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; – располагает конфиденциальными данными, к которым имеет доступ.	Сотрудники, обрабатывающие ПДн
3	Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам	– обладает всеми возможностями лиц первой и второй категорий; – располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной систем, через которую он осуществляет доступ, и составе технических средств ИСПДн; – имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.	Отсутствует
4	Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; – обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; – имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; – имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; – обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.	Отсутствует
5	Зарегистрированные пользователи с полномочиями системного администратора	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;	Системный администратор ИСПДн

	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.	
6	Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн	– обладает всеми возможностями лиц предыдущих категорий; – обладает полной информацией об ИСПДн; – имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; – не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	Отсутствует
7	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	– обладает информацией об алгоритмах и программах обработки информации на ИСПДн; – обладает возможностями внесения ошибок, недеklarированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.	Отсутствует
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	– обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; – может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.	Системный администратор ИСПДн

6.5. Предположения о возможностях нарушителя.

6.5.1. Для получения исходных данных о ИСПДн нарушитель может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования, а также по локальным сетям ИСПДн. Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления. Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

6.5.2. В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

6.5.3. Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

6.6. Предположения об имеющихся у нарушителя средствах атак.

6.6.1. Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

6.6.2. Внешний нарушитель может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;
- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

6.6.3. Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

6.7. Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
- бумажные носители информации;
- штатные программно-аппаратные средства ИСПДн;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
- незащищенные каналы связи.

6.8. Для снижения опасности реализации актуальных необходимо:

- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;
- разработка инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты;
- постоянное обновление антивирусных баз.