|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ  Генеральный директор ООО «ВЛАДЕЛЕЦ ИСПДН»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Модель угроз безопасности** **информации**

**Информационной системы персональных данных**

**«ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

Оглавление

[Термины и определения 3](#_Toc158383205)

[Список принятых сокращений 13](#_Toc158383206)

[1. Общие положения 15](#_Toc158383207)

[2. Описание системы и ее характеристика как объекта защиты 18](#_Toc158383208)

[2.1 Наименование системы 18](#_Toc158383209)

[2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных 18](#_Toc158383210)

[2.3 Назначение, задачи (функции) системы, состав обрабатываемой информации и ее правовой режим 18](#_Toc158383211)

[2.4 Основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создается (функционирует) система 19](#_Toc158383212)

[2.5 Состав и архитектура системы 19](#_Toc158383213)

[2.5.1. Структура системы 19](#_Toc158383214)

[2.5.2 Архитектура системы 20](#_Toc158383215)

[2.5.3 Состав системы 21](#_Toc158383216)

[2.6 Описание групп внешних и внутренних пользователей системы, уровней их полномочий и типов доступа 23](#_Toc158383217)

[2.7 Описание внешних интерфейсов и взаимодействий системы с пользователями 24](#_Toc158383218)

[3 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации 25](#_Toc158383219)

[4 Возможные объекты воздействия угроз безопасности информации 27](#_Toc158383220)

[5 Источники угроз безопасности информации 32](#_Toc158383221)

[5.1 Характеристика нарушителей 32](#_Toc158383222)

[5.2 Категория нарушителей 41](#_Toc158383223)

[5.3 Определение актуальных нарушителей при реализации УБИ 46](#_Toc158383224)

[6 Способы реализации (возникновения) угроз безопасности информации 48](#_Toc158383225)

[7 Актуальные угрозы безопасности информации 54](#_Toc158383226)

[7.1 Определение возможных угроз безопасности информации 54](#_Toc158383227)

[7.2 Сценарии реализации и выводы об актуальности угроз 54](#_Toc158383228)

[7.3 Вывод об актуальности угроз 55](#_Toc158383229)

[Заключение 57](#_Toc158383230)

# Термины и определения

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

**Автоматизированная система в защищенном исполнении (АСЗИ) –** автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

**Адекватность –** свойство соответствия преднамеренному поведению и результатам.

**Архитектура систем и сетей -** совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

**Атака –** целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность** – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

**Безопасность персональных данных** - состояние защищенности 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.

**Взаимодействующая (смежная) система -** система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с системой и сетью оператора и не включена им в границу процесса оценки угроз безопасности информации.

**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.

**Возможности нарушителя** - мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

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

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Встраивание криптосредства** – процесс подключения криптосредства к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции

**Граница оценки угроз безопасности информации -** совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности).

**Документированные (декларированные) возможности ПО (ТС) –** функциональные возможности ПО (ТС), описанные в документации на ПО (ТС).

**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.

**Доступность информации** - состояние информации, характеризуемое способностью автоматизированной системы обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

**Жизненно важные интересы** – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

**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.

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

**Инсталляция** – установка программного продукта на компьютер. Инсталляция обычно выполняется под управлением инсталлятора – программы, которая приводит состав и структуру устанавливаемого программного изделия в соответствии с конфигурацией компьютера, а также настраивает программные параметры согласно типу имеющейся операционной системы, классам решаемых задач и режимам работы. Таким образом, инсталляция делает программный продукт пригодным для использования в данной вычислительной системе и готовым решать определенный класс задач в определенном режиме работы.

**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.

**Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

**Информационно-телекоммуникационная сеть общего пользования** – информационно-телекоммуникационная сеть, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

**Информационные ресурсы -** информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Канал атаки** – среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки.

**Компонент (системы, сети) -** программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей.

**Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей Организации и посторонних транспортных, технических и иных материальных средств.

**Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

**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.

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

**Криптографически опасная информация (КОИ) –** информация о состояниях криптосредства, знание которой нарушителем позволит ему строить алгоритмы определения ключевой информации (или ее части) или алгоритмы бесключевого чтения.

**Криптосредство –** шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

**Межсетевой экран -** локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Модель нарушителя** – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

**Модель угроз** – перечень возможных угроз 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.

**Негативные функциональные возможности** – документированные и недокументированных возможности программных и аппаратных компонентов криптосредства и среды функционирования криптосредства, позволяющие:

- модифицировать или искажать алгоритм работы криптосредств в процессе их использования;

- модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием криптосредства;

получать доступ нарушителям к хранящимся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации, а также к защищаемой информации.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно Нарушение конфиденциальности персональных данных, 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.

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

**Обеспечивающие системы** - инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

**Обладатель информации -** лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

**Обработка персональных данных -** действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Опубликованные возможности ПО или ТС** – возможности, сведения о которых содержатся в общедоступных открытых источниках (технические и любые другие материалы разработчика ПО или ТС, монографии, публикации в СМИ, материалы конференций и других форумов, информация из сети Internet и т.д.)

**Основные (критические) процессы (бизнес-процессы)** - управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**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.

**Поставщик услуг -** лицо, предоставляющее оператору и (или) обладателю на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

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

**Программная закладка** - код программы, преднамеренно внесенный программу с целью осуществить утечку, изменить, блокировать, уничтожать информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программно-аппаратное средство -** устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

**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.

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

**Сеть Интернет** - всемирная система объединенных компьютерных сетей для хранения и передачи информации.

**Сайт в сети Интернет** - совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединенных под одним адресом (доменным именем или IP-адресом).

**Специальная защита** – комплекс организационных и технических мероприятий, обеспечивающих защиту информации от утечки по каналам побочных излучений и наводок.

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

**Среда функционирования средств криптографической защиты информации** -совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

**Средства имитозащиты** - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

**Средства кодирования** - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

**Средства криптографической защиты информации** - средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

**Средства шифрования** - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

**Средства электронной подписи** - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

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

**Технические средства информационной системы персональных данных -** средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**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 невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Уполномоченное оператором лицо** - лицо, которому на основании договора оператор поручает обработку персональных данных.

**Уровень криптографической защиты информации** – совокупность требований, предъявляемых к криптосредству.

**Успешная атака** – атака, достигшая своей цели.

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

**Уполномоченное оператором лицо** – лицо, которому на основании договора оператор поручает обработку персональных данных.

**Учетность** – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

**Уязвимость -**недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

**Характеристика безопасности объекта** – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

**Целостность информации** - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность персональных данных при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

# Список принятых сокращений

|  |  |
| --- | --- |
| АСУ ТП | Автоматизированная система управления технологическими процессами |
| АРМ | Автоматизированное рабочее место |
| БД | База данных |
| ВМ | Виртуальная машина |
| ГОСТ | Государственный стандарт |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| ПАО | Публичное акционерное общество |
| ПО | Программное обеспечение |
| СКЗИ | Средство криптографической защиты информации |
| СУБД | Система управления базами данных |
| УБИ | Угроза безопасности информации |
| ФСБ | Федеральная служба безопасности |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |
| ЦОД | Центр обработки данных |
| AMQP | Advanced Message Queuing Protocol, открытый протокол прикладного уровня для передачи сообщений между компонентами системы |
| API | Application Program Interface, интерфейс прикладного программирования |
| ARP | Address Resolution Protocol, протокол определения адреса — протокол в компьютерных сетях, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу |
| BIOS | Basic input/output system, базовая система ввода-вывода |
| CIM XML | Формат для обмена XML-данными |
| Cookies-файл | небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя |
| DNS | Domain Name System, «система доменных имён» — компьютерная распределённая система для получения информации о доменах |
| HTTP | HyperText Transfer Protocol, «протокол передачи гипертекста», протокол прикладного уровня передачи данных |
| HTTPS | HyperText Transfer Protocol Secure, расширение протокола HTTP для поддержки шифрования в целях повышения безопасности |
| ID | Identifier, data name, идентифика́тор — уникальный признак объекта, позволяющий отличать его от других объектов, то есть идентифицировать |
| IoT | Internet of things, Интернет вещей - концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой |
| RDP | Remote Desktop Protocol, протокол удалённого рабочего стола, проприетарный протокол прикладного уровня |
| SQL | Structured Query Language, это язык запросов, который применяют, чтобы работать с базами данных, структурированных особым образом |
| SSH | Secure Shell, [сетевой протокол прикладного уровня](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F) |
| TELNET | Teletype Network, сетевой протокол для реализации текстового терминального интерфейса по сети (в современной форме — при помощи транспорта TCP) |
| Telnet-порт | Реализация клиентской части протокола TELNET |
| TCP/IP | Transmission Control Protocol/Internet Protocol сетевая модель передачи данных |
| UEFI | Unified Extensible Firmware Interface, интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования |
| URI | Uniform Resource Identifier, унифицированный (единообразный) идентификатор ресурса |
| USB | Universal Serial Bus, «универсальная последовательная шина» — последовательный интерфейс для подключения периферийных устройств к вычислительной технике |
| XML | eXtensible Markup Language - Расширяемый язык разметки |

# 1. Общие положения

Модель угроз безопасности информации Информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее - Модель угроз) содержит описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее – ИСПДн «ВЛАДЕЛЕЦ ИСПДН» или ИС).

Целью моделирования угроз безопасности информации является выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности, обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств её обработки), а также к нарушению или прекращению функционирования систем и сетей. В качестве угроз безопасности информации, подлежащих определению при моделировании угроз безопасности информации, рассматриваются неправомерные действия и (или) воздействия на информационные ресурсы или компоненты систем или сетей, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

- инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

- определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

- оценка способов реализации (возникновения) угроз безопасности информации;

- оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

- оценка сценариев реализации угроз безопасности информации в системах и сетях.

Оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания ИС, так и в ходе ее эксплуатации, в том числе при развитии (модернизации). Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов ИС. Учет изменений угроз безопасности информации обеспечит своевременную выработку адекватных и эффективных мер по защите информации (обеспечению безопасности) в ИС.

Модель угроз разработана обществом с ограниченной ответственностью ООО «ОРГАН ПО АТТЕСТАЦИИ» в соответствии с договором между ООО «ВЛАДЕЛЕЦ ИСПДН» и ООО «ОРГАН ПО АТТЕСТАЦИИ».

Модель угроз разработана в соответствии с методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021 и использует банк данных угроз безопасности информации, сформированный ФСТЭК России (bdu.fstec.ru) и актуальный на момент проведения обследования (27.02.2024).

В Модели используются термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования ИС.

Изменение модели угроз безопасности информации осуществляется в случаях:

- изменения требований нормативных правовых актов Российской Федерации, методических документов ФСТЭК России, регламентирующих вопросы оценки угроз безопасности информации;

- изменений архитектуры и условий функционирования ИС, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;

- выявления, в том числе по результатам контроля уровня защищенности ИС и содержащейся в ней информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;

- включения в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

Наименование предприятий разработчика и заказчика системы и их реквизиты:

**Генеральный заказчик – Общество с ограниченной ответственностью «ВЛАДЕЛЕЦ ИСПДН» (далее – ООО «ВЛАДЕЛЕЦ ИСПДН», Общество):**

- Местонахождение:

- ИНН

**Подрядчик (Разработчик, Исполнитель работ) – общество с ограниченной ответственностью «Орган по аттестации» (ООО «ОРГАН ПО АТТЕСТАЦИИ»):**

- Местонахождение:

- ИНН

- лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации, рег;

- лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) рег.

# 2. Описание системы и ее характеристика как объекта защиты

## 2.1 Наименование системы

* Информационная система персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН»;
* ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

## 2.2 Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных

По результатам установления уровня защищенности персональных данных ИС в соответствии с документом «*Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденном постановлением Правительства Российской Федерации от 01.11.2012 № 1119*, установлена необходимость обеспечения **3-го уровня** защищенности персональных данных. Результаты установления уровня защищенности персональных данных ИС приведены в документе *«АКТ определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» и утвержденном Генеральным директором ООО «ВЛАДЕЛЕЦ ИСПДН» в 2024*.

## 2.3 Назначение, задачи (функции) системы, состав обрабатываемой информации и ее правовой режим

ИС функционирует в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и иных нормативно – правовых актов законодательства РФ. ИС создана для обеспечения автоматизации обработки персональных данных с помощью средств вычислительной техники.

В ИС обрабатывается следующий состав персональных данных в рамках автоматизированной обработки:

- Фамилия;

- Имя;

- Отчество;

- Дата рождения;

- Пол;

- Сведения о трудовом стаже.

Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) не осуществляется.

Оператором не осуществляется обработка специальных категорий персональных данных, в автоматизированном виде, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

## 2.4 Основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создается (функционирует) система

Обработка персональных данных в ИСПДн производится в целях:

- осуществление деятельности в соответствии с Уставом Общества;

- оформление трудовых отношений, ведение кадрового и бухгалтерского учёта, оформление гражданско-правовых отношений;

- в иных законных целях.

Для организации и контроля за работой пользователей, а также контроля корректного функционирования программного обеспечения, технических средств и средств защиты информации на объекте информатизации назначены специалисты, обладающие административными полномочиями. Функции, права, обязанности и порядок работы администраторов регламентируются разработанными в организации инструкциями, а также руководящими документами ФСТЭК и ФСБ России.

## 2.5 Состав и архитектура системы

### 2.5.1. Структура системы

ИСПДн «ВЛАДЕЛЕЦ ИСПДН» состоит из одного АРМ на базе ПЭВМ, подключенного к сети Интернет через ЛВС Общества (см. рисунок 1):

### 2.5.2 Архитектура системы

Архитектура ИС представляет собой совокупность программных и программно-аппаратных средств, содержащую следующие компоненты, обеспечивающие функционирование ИС:

а) программные средства:

– базовая система ввода-вывода программно-технических средств (BIOS);

– системное программное обеспечение (операционная система);

– общесистемное программное обеспечение (ОСПО - утилиты и драйверы системного обеспечения, включая утилиты и драйверы управления аппаратными ресурсами);

– специальное программное обеспечение (СПО), на базе которого реализуется основной функционал ИС.

б) штатные механизмы защиты программно-технических средств:

– средства идентификации и аутентификации пользователей;

– средства управления доступом пользователей;

– средства обеспечения регистрации и учета действий пользователей.

в) каналы информационного взаимодействия:

– телекоммуникационное оборудование ИС

### 2.5.3 Состав системы

Состав комплекса программно-технических средств ИС приведен в таблице 1, состав сетевого и коммутационного оборудования ИС – в таблице 2, состав общесистемного и прикладного программного обеспечения – в таблице 3, состав средств защиты информации приведен в таблице 4.

Таблица 1 –компоненты ИСПДн

| **Показатель** | **Значение** |
| --- | --- |
| **Количественные характеристики ИСПДн** | |
| Серверные компоненты | Отсутствуют |
| Клиентские компоненты | 1 (одно) автоматизированное рабочее место (АРМ) на базе ПЭВМ без среды виртуализации |
| **Качественные характеристики клиентских компонентов** | |
| Аппаратная платформа | Intel (Intel(R) Core(TM) i5-4200U CPU @ 1.60GHz 2.30 GHz) |
| Форм-фактор аппаратной платформы | Ноутбук |
| Среда виртуализации | Не используется |
| Сегментирование | Не используется |
| Операционная система | Windows 10 Pro (19045.4046) |
| Система хранения данных | Внутренний жесткий диск |
| Общесистемное программное обеспечение (ОСПО) | Будет уточняться на этапе проектирования |
| Специальное программное обеспечение (СПО) | Microsoft Office 2016 |
| Используемые средства защиты | Штатные средства операционной системы (ОС) |

Таблица 2 - Телекоммуникационное оборудование

| **Тип оборудования** | **Наименование** | **Версия** |
| --- | --- | --- |
| Маршрутизатор | Keenetic Viva | 4.07 |

Таблица 3 – Состав общесистемного и прикладного программного обеспечения

| **Тип программного обеспечения** | **Наименование** | **Версия** |
| --- | --- | --- |
| Операционная система | Windows | 10 Pro |
| Пакет офисных программ | Microsoft Office | 2016 |

Таблица 4 – Состав средств защиты информации

| **Тип средства** | **Наименование и основная (мажорная) версия** | **Сведения**  **о сертификате** |
| --- | --- | --- |
| - | - | - |

## 2.6 Описание групп внешних и внутренних пользователей системы, уровней их полномочий и типов доступа

Предоставление доступа к техническим средствам, информационным ресурсам, в том числе к защищаемой информации, регламентировано локальными нормативно-правовыми актами Общества и осуществляется на основании соответствующих распоряжений должностных лиц.

Пользователи, обладающие правом доступа к защищаемой информации, подлежат регистрации в соответствующих реестрах и базах данных на основе сопоставления их идентификационных данных уникальным учетным записям, и могут быть объединены в группы.

Перечень типовых функций и обязанностей различных категорий пользователей регламентирован локальными руководящими документами Общества, при этом пользователи обладают различающимися правами по доступу к защищаемой информации.

1. В ИС предусмотрены следующие группы внутренних пользователей системы:
   1. привилегированные внутренние пользователи (работники Общества):
      1. должностные лица, ответственные за контроль над процессами обеспечения информационной безопасности и штатного функционирования информационных систем (администратор информационной безопасности (ИБ));
      2. лица, должностными обязанностями которых является обеспечение штатного функционирования (поддержание работоспособности и иные виды технического обслуживания (администраторы информационных систем, телекоммуникационного оборудования, систем управления базами данных и программного обеспечения) (системный администратор);
      3. должностные лица, ответственные за организацию и осуществление контроля над порядком обработки информации ограниченного доступа;
      4. иные лица, временно обладающие привилегированным доступом к информационным ресурсам ИС, предоставленным установленным порядком ввиду временного исполнения ими должностных обязанностей;
   2. непривилегированные внутренние пользователи (работники Общества):
      1. лица, должностными обязанностями которых является обеспечение обработки персональных данных и осуществляющие работу с АРМ путем подключения к ИС (исполнитель и пр.);
2. Цели и задачи обработки информации в ИС не предполагают наличие внешних пользователей (пользователей, не являющихся работниками оператора).

## 2.7 Описание внешних интерфейсов и взаимодействий системы с пользователями

Внутренние пользователи (авторизованные пользователи ИС), являющиеся сотрудниками оператора, осуществляют работу с ИС посредством использования на АРМ персонала оператора, расположенных в пределах контролируемой зоны Общества, с использованием клиентского ПО.

# 3 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

В ходе оценки угроз безопасности информации определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

Возможные негативные последствия от реализации угроз безопасности информации определены как на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, так и на основе информации, представляемой профильными подразделениями и специалистами обладателя информации.

В соответствии с методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021, исходными данными для определения негативных последствий от реализации угроз безопасности информации являются:

* общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;
* нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;
* документация на сети и системы (в части сведений о назначении и функциях систем и сетей, о составе и архитектуре систем и сетей);
* технологические, производственные карты или иные документы, содержащие описание основных (критических) процессов (бизнес-процессов) обладателя информации, оператора;
* результаты оценки рисков (ущерба), проведенной обладателем информации или оператором.

Актуальные для Общества виды рисков (ущерба) и описание возможных негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации в ИС может привести к возникновению рисков (ущерба), представлены в таблице 6.

**Таблица 6 - Виды рисков (ущерба) и возможные негативные последствия**

| **№** | **Виды риска (ущерба)** | **Возможные типовые негативные последствия** |
| --- | --- | --- |
| У1 | Ущерб физическому лицу | Нарушение конфиденциальности (утечка) персональных данных. |
| Разглашение персональных данных граждан. |
| У2 | Ущерб юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью | Нарушение законодательства Российской Федерации |
| Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) |
| Необходимость дополнительных (незапланированных) затрат на восстановление деятельности |
| Нарушение деловой репутации |
| Утрата доверия |
| Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) |
| Простой информационной системы или сети |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) |

# 4 Возможные объекты воздействия угроз безопасности информации

Возможными объектами воздействия УБИ для ИС могут являться:

‒ защищаемая информация в ИС;

‒ программные средства (системное и прикладное ПО, системы виртуализации, виртуальные сервера);

‒ программно-аппаратные средства обработки и хранения информации (АРМ, серверы, мобильные устройства);

‒ машинные носители информации;

‒ телекоммуникационное оборудование и каналы связи;

‒ средства защиты информации;

‒ обеспечивающие системы.

Основными видами воздействий УБИ являются:

* утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
* несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
* отказ в обслуживании программных средств (нарушение доступности);
* несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
* несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
* нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

    Объекты воздействия УБИ для ИС и виды воздействия на них представлены в таблице 7.

**Таблица 7 – Объекты воздействия и виды воздействия на них**

| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| --- | --- | --- |
| Нарушение конфиденциальности (утечка) персональных данных (У1) | Защищаемая информация в ИС | Несанкционированный доступ к компонентам, защищаемой информации |
| Программные средства | Несанкционированный доступ к компонентам, защищаемой информации |
| Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к компонентам, защищаемой информации |
| Машинные носители информации | Несанкционированный доступ к компонентам, защищаемой информации |
| Телекоммуникационное оборудование и каналы связи | Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности) |
| Пользователи ИС | Несанкционированный доступ к защищаемой информации |
| Разглашение персональных данных граждан (У1) | Защищаемая информация в ИС | Несанкционированный доступ к компонентам, защищаемой информации |
| Программные средства | Несанкционированный доступ к компонентам, защищаемой информации |
| Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к компонентам, защищаемой информации |
| Машинные носители информации | Несанкционированный доступ к компонентам, защищаемой информации |
| Телекоммуникационное оборудование и каналы связи | Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности) |
| Пользователи ИС | Несанкционированный доступ к защищаемой информации |
| Нарушение законодательства Российской Федерации (У2) | Защищаемая информация в ИС | Несанкционированный доступ к защищаемой информации |
| Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности) |
| Несанкционированная модификация, подмена, искажение защищаемой информации (нарушение целостности) |
| Программно-аппаратные средства обработки и хранения информации | Несанкционированное использование вычислительных ресурсов ИС в интересах решения несвойственных им задач |
| Программные средства | Несанкционированное использование вычислительных ресурсов ИС в интересах решения несвойственных им задач |
| Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) (У2) | Защищаемая информация в ИС | Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) |
| Программно-аппаратные средства обработки и хранения информации | Нарушение функционирования (работоспособности) программно-аппаратных средств обработки и хранения информации |
| Программные средства | Отказ в обслуживании программных средств (нарушение доступности) |
| Телекоммуникационное оборудование и каналы связи | Нарушение функционирования (работоспособности) телекоммуникационного оборудования |
| Машинные носители информации | Нарушение функционирования (работоспособности) машинных носителей |
| Необходимость дополнительных (незапланированных) затрат на восстановление деятельности (У2) | Защищаемая информация в ИС | Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) |
| Программно-аппаратные средства обработки и хранения информации | Нарушение функционирования (работоспособности) программно-аппаратных средств обработки и хранения информации |
| Программные средства | Отказ в обслуживании программных средств (нарушение доступности) |
| Телекоммуникационное оборудование и каналы связи | Нарушение функционирования (работоспособности) телекоммуникационного оборудования |
| Машинные носители информации | Нарушение функционирования (работоспособности) машинных носителей |
| Нарушение деловой репутации (У2) | Пользователи ИС | Несанкционированный доступ к защищаемой информации |
| Утрата доверия (У2) | Защищаемая информация в ИС | Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) |
| Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) (У2) | Защищаемая информация в ИС | Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности) |
| Программно-аппаратные средства обработки и хранения информации | Нарушение функционирования (работоспособности) программно-аппаратных средств обработки и хранения информации |
| Программные средства | Отказ в обслуживании программных средств (нарушение доступности) |
| Телекоммуникационное оборудование и каналы связи | Нарушение функционирования (работоспособности) телекоммуникационного оборудования |
| Машинные носители информации | Нарушение функционирования (работоспособности) машинных носителей |
| Простой информационной системы или сети | Защищаемая информация в ИС | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Программные средства | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Машинные носители информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Телекоммуникационное оборудование и каналы связи | Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности) |
| Средства защиты информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Пользователи ИС | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2) | Защищаемая информация в ИС | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Программные средства | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Машинные носители информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Телекоммуникационное оборудование и каналы связи | Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности) |
| Средства защиты информации | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |
| Пользователи ИС | Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данных |

# 5 Источники угроз безопасности информации

## 5.1 Характеристика нарушителей

В ходе оценки угроз безопасности информации определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей, – актуальные нарушители.

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для ИС.

В соответствии с «Методикой оценки угроз безопасности информации» основными видами нарушителей, подлежащих оценке, являются:

* специальные службы иностранных государств;
* террористические, экстремистские группировки;
* преступные группы (криминальные структуры);
* отдельные физические лица (хакеры);
* конкурирующие организации;
* разработчики программных, программно-аппаратных средств;
* лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
* поставщики услуг связи, вычислительных услуг;
* лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
* лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
* авторизованные пользователи систем и сетей;
* системные администраторы и администраторы безопасности;
* бывшие (уволенные) работники (пользователи).

Нарушители признаются актуальными для ИС, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для ИС негативным последствиям и соответствующим рискам (видам ущерба). Возможные цели реализации угроз безопасности информации нарушителями и оценка применимости вида нарушителя приведены в таблице 8.

Таблица 8 – Виды нарушителей и цели реализации угроз безопасности информации

| **№ вида** | **Виды нарушителей** | **Категория нарушителя** | **Возможные цели реализации УБИ** | **Оценка применимости вида нарушителя** |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
|  | Специальные службы иностранных государств | Внешний | Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса | Неприменимо.  Не имеют достаточной мотивации для осуществления деятельности в отношении Общества по нанесению ущерба государству, отдельным его сферам деятельности или секторам экономики, дискредитации или дестабилизации деятельности органов государственной власти, организаций, получения конкурентных преимуществ на уровне государства, срыва заключения международных договоров, создания внутриполитического кризиса. Следовательно, наступление указанных событий невозможно при реализации угроз безопасности информации в отношении Общества. |
|  | Террористические, экстремистские группировки | Внешний | Совершение террористических актов, угроза жизни граждан.  Нанесение ущерба отдельным сферам деятельности или секторам экономики государства.  Дестабилизация общества.  Дестабилизация деятельности органов государственной власти, организаций | Неприменимо.  Не имеют достаточной мотивации для осуществления деятельности в отношении Общества по нанесению ущерба государству, отдельным его сферам деятельности или секторам экономики, совершению террористических актов, угрозе жизни граждан, по преследованию идеологических или политических мотивов, дестабилизации деятельности органов государственной власти, организаций, дестабилизации общества. Следовательно, наступление указанных событий невозможно при реализации угроз безопасности информации в отношении Общества. |
|  | Преступные группы (криминальные структуры)[[1]](#footnote-2) | Внешний | Получение финансовой или иной материальной выгоды.  Желание самореализации (подтверждение статуса) | Применимо.  Возможно вхождение данного типа нарушителя в сговор с внутренними нарушителями с целями, указанными в столбце 4. |
|  | Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса) | Применимо.  Возможно вхождение данного типа нарушителя в сговор с внутренними нарушителями с целями, указанными в столбце 4. |
|  | Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды | Применимо.  Возможно вхождение данного типа нарушителя в сговор с внутренними нарушителями с целями, указанными в столбце 4. |
|  | Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем | Внешний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ | Неприменимо.  Для поставки средств привлекаются известные на рынке Общества исходя из условия наличия у них подтвержденного опыта, обладающие положительной репутацией и действующими лицензиями ФСТЭК России при проведении работ или оказания услуг по технической по защите информации и ФСБ России по разработке, производству, распространению шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем. |
|  | Разработчики программных, программно-аппаратных средств | Внутренний | Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки.  Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия | Неприменимо.  Разработчики программных, программно-аппаратных средств ИС не заинтересованы в преднамеренном внесении недекларированных возможностей ввиду недостаточности мотивации. Мотивацию разработчиков на преднамеренное внесение недекларированных возможностей следует считать достаточной только в случае сговора со специальными службами иностранных государств, которые исключены из числа актуальных нарушителей, при этом в качестве цели может рассматриваться получение финансовой прибыли.  Кроме того, отдельные категории разработчиков программных, программно-аппаратных средств АРМ ИС, могут бы исключены из числа потенциальных нарушителей безопасности информации в случае, если деятельность в области разработки является лицензируемым видом деятельности (таким, например, как разработка и производство средств защиты информации). Также программные или программно-аппаратные средства ИС, являющиеся результатом разработки, подлежат проверке соответствия предъявляемым к ним требованиям в форме сертификации, устанавливаемой согласно положениям постановления Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации». |
|  | Поставщики вычислительных услуг, услуг связи | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ | Неприменимо.  В отношении работников третьих лиц, привлекаемых по договорам как поставщиков услуг связи, вычислительных услуг используются следующие меры:   * Общества привлекаются только на основании договора, включающего соглашения о неразглашении конфиденциальной информации; * для проведения работ привлекаются известные на рынке Общества исходя из условия наличия у них подтвержденного опыта и обладающие положительной репутацией; * для проведения работ привлекаются Общества, обладающие лицензиями ФСТЭК России и ФСБ России (при необходимости проведения работ по защите информации); * представителям третьих лиц передается информация, предоставляются права и назначаются привилегии в объеме, необходимом только для выполнения ими договорных работ; * все работы проводятся только под строгим контролем работников Общества. |
|  | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия | Применимо.  В помещение, где располагаются программно-технические средства ИС, имеют доступ обслуживающий персонал (администрация, охрана, уборщики и т.д.), поэтому вероятны реализации угроз безопасности информации с целями, указанными в столбце 4. |
|  | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.  Получение конкурентных преимуществ | Применимо.  В помещения, где располагаются программно-технические средства ИС, имеют доступ указанные в столбце 2 лица, поэтому вероятны реализации угроз безопасности информации с целями, указанными в столбце 4. |
|  | Авторизованные пользователи систем и сетей | Внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса).  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия | Применимо.  Пользователи ИС имеют непосредственный доступ в помещение, где располагаются программно-технические средства ИС, поэтому вероятны реализации угроз безопасности информации с целями, указанными в столбце 4. |
|  | Системные администраторы и администраторы безопасности | Внутренний | Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса).  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия | Применимо.  Вероятны реализации угроз безопасности информации с целями, указанными в столбце 4. |
|  | Бывшие работники (пользователи) | Внешний | Получение финансовой или иной материальной выгоды.  Месть за ранее совершенные действия | Применимо.  Ввиду возможных реорганизаций и оптимизации деятельности Общества возможны появления недовольных бывших пользователей ИС, поэтому вероятны реализации угроз безопасности информации с целями, указанными в столбце 4. |

Для повышения уровня своих возможностей нарушители вида 3, 4, 13 могут вступать в сговор с нарушителями 9, 10, 11, 12 видов.

Соответствие нарушителей, возможных целей реализации ими угроз безопасности и возможных негативных последствий и видов рисков (ущербов) от их реализации (возникновения) приведено в таблице 9.

Таблица 9 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

| **№ п/п** | **Виды нарушителей** | **Возможные цели реализации угроз безопасности информации** | | **Соответствие целей видам риска (ущерба) и возможным негативным последствиям** |
| --- | --- | --- | --- | --- |
| **Нанесение ущерба физическому лицу** | **Нанесение ущерба юридическому лицу** |
|  | Преступные группы (криминальные структуры) | \_ | Получение финансовой или иной материальной выгоды.  Желание самореализации (подтверждение статуса) | У1  Нарушение конфиденциальности (утечка) персональных данных.  Разглашение персональных данных граждан.  У2  Нарушение законодательства Российской Федерации  Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)  Необходимость дополнительных (незапланированных) затрат на восстановление деятельности  Нарушение деловой репутации  Утрата доверия  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)  Простой информационной системы или сети  Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) |
|  | Отдельные физические лица (хакеры) | Любопытство или желание самореализации (подтверждение статуса) | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации (подтверждение статуса) |
|  | Конкурирующие организации | - | Получение конкурентных преимуществ. |
|  | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | - | Получение финансовой или иной материальной выгоды.  Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | - | Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Авторизованные пользователи систем и сетей | Любопытство или желание самореализации.  Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации. |
|  | Системные администраторы и администраторы безопасности | Месть за ранее совершенные действия.  Непреднамеренные, неосторожные или неквалифицированные действия | Получение финансовой или иной материальной выгоды.  Любопытство или желание самореализации.  Непреднамеренные, неосторожные или неквалифицированные действия |
|  | Бывшие (уволенные) работники (пользователи) | Месть за ранее совершенные действия | Получение финансовой или иной материальной выгоды.  Месть за ранее совершенные действия |

## 5.2 Категория нарушителей

Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

* базовыми возможностями по реализации угроз безопасности информации (Н1);
* базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
* средними возможностями по реализации угроз безопасности информации (Н3);
* высокими возможностями по реализации угроз безопасности информации (Н4).

Уровни возможностей нарушителей по реализации угроз безопасности информации приведены в таблице 10.

Таблица 10 – Уровни возможностей нарушителей по реализации угроз безопасности информации

| **№** | **Уровень возможностей нарушителей** | **Возможности нарушителей по реализации угроз безопасности информации** | **Виды нарушителей** |
| --- | --- | --- | --- |
|  | Нарушитель, обладающий базовыми возможностями | Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты.  Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов.  Обладает базовыми компьютерными знаниями и навыками на уровне пользователя.  Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним.  **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов** | Физическое лицо (хакер)  Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем  Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.)  Авторизованные пользователи систем и сетей  Бывшие работники (пользователи) |
|  | Нарушитель, обладающий базовыми повышенными возможностями | Обладает всеми возможностями нарушителей с базовыми возможностями.  Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз.  Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей.  Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации.  Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.  **Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей** | Преступные группы (два лица и более, действующие по единому плану)  Конкурирующие организации  Поставщики вычислительных услуг, услуг связи  Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ  Системные администраторы и администраторы безопасности |
|  | Нарушитель, обладающий средними возможностями | Обладает всеми возможностями нарушителей с базовыми повышенными возможностями.  Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей).  Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей).  Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств.  Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа.  Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях.  Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах.  Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц.  **Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей** | Террористические, экстремистские группировки  Разработчики программных, программно-аппаратных средств |
|  | Нарушитель, обладающий высокими возможностями | Обладает всеми возможностями нарушителей со средними возможностями.  Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня».  Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств.  Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение.  Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности.  Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.  Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации.  Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей.  **Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей** | Специальные службы иностранных государств |

## 5.3 Определение актуальных нарушителей при реализации УБИ

Для актуальных нарушителей определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования ИС, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории:

* внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
* внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Определение актуальных нарушителей при реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности представлены в таблице 11.

Таблица 11 – Актуальные нарушители при реализации угроз безопасности информации и соответствующие им возможности

| **№**  **п/п** | **Виды риска (ущерба) и возможные негативные последствия** | **Виды актуального нарушителя** | **Категория нарушителя** | **Уровень возможностей нарушителя** |
| --- | --- | --- | --- | --- |
|  | У1: Нарушение конфиденциальности (утечка) персональных данных.  Разглашение персональных данных граждан. | Отдельные физические лица (хакеры) | Внешний  Внутренний[[2]](#footnote-3) | Н2 |
| Авторизованные пользователи систем и сетей | Внутренний | Н1 |
| Системные администраторы и администраторы безопасности | Внутренний | Н2 |
| Бывшие (уволенные) работники (пользователи) | Внешний | Н1 |
|  | У2: Нарушение законодательства Российской Федерации  Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)  Необходимость дополнительных (незапланированных) затрат на восстановление деятельности  Нарушение деловой репутации  Утрата доверия  Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)  Простой информационной системы или сети  Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) | Преступные группы (криминальные структуры) | Внешний  Внутренний3 | Н2 |
| Отдельные физические лица (хакеры) | Внешний  Внутренний3 | Н2 |
| Конкурирующие организации | Внешний  Внутренний3 | Н2 |
| Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ | Внутренний | Н2 |
| Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Н1 |
| Авторизованные пользователи систем и сетей | Внутренний | Н1 |
| Системные администраторы и администраторы безопасности | Внутренний | Н2 |
| Бывшие работники (пользователи) | Внешний | Н1 |

# 6 Способы реализации (возникновения) угроз безопасности информации

В ходе оценки угроз безопасности информации определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ИС – актуальные способы реализации (возникновения) угроз безопасности информации.

Основными способами реализации (возникновения) угроз безопасности информации являются:

* использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);
* внедрение вредоносного программного обеспечения;
* использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
* установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;
* формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
* перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
* инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
* нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
* ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

* внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
* интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;
* интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
* возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в таблице 12.

В таблице 12 приведены объекты воздействия, являющиеся актуальными для ИС и определённые в таблице 7.

Таблица 12 – Актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

| **№**  **п/п** | **Вид нарушителя** | **Категория нарушителя** | **Объект воздействия** | **Доступные интерфейсы** | **Способы реализации** |
| --- | --- | --- | --- | --- | --- |
|  | Преступные группы (криминальные структуры) (Н2) | Внешний  Внутренний3 | Защищаемая информация в ИС  Программные средства  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных |
|  | Отдельные физические лица (хакеры) (Н1) | Внешний  Внутренний3 | Защищаемая информация в ИС  Программные средства  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных |
|  | Конкурирующие организации | Внешний  Внутренний3 | Защищаемая информация в ИС  Программные средства  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных |
|  | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) (Н1) | Внутренний | Защищаемая информация в ИС  Программные средства  Программно-аппаратные средства обработки и хранения информации  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы.  Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Непреднамеренные, неосторожные или неквалифицированные действия в ходе обслуживания инфраструктуры |
|  | Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (Н2) | Внутренний | Защищаемая информация в ИС  Программные средства  Программно-аппаратные средства обработки и хранения информации  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных  Непреднамеренные, неосторожные или неквалифицированные действия в ходе эксплуатации, ремонта |
|  | Авторизованные пользователи систем и сетей (Н1) | Внутренний | Защищаемая информация в ИС  Программные средства  Программно-аппаратные средства обработки и хранения информации  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Интерфейсы для пользователей.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы.  Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования | Непреднамеренные, неосторожные или неквалифицированные действия в ходе эксплуатации системы |
|  | Системные администраторы и администраторы безопасности (Н2) | Внутренний | Защищаемая информация в ИС  Программные средства  Программно-аппаратные средства обработки и хранения информации  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы.  Интерфейсы для использования съемных машинных носителей информации и периферийного оборудования. | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных  Непреднамеренные, неосторожные или неквалифицированные действия в ходе настройки и эксплуатации |
|  | Бывшие работники (пользователи) (Н1) | Внешний | Защищаемая информация в ИС  Программные средства  Телекоммуникационное оборудование и каналы связи  Средства защиты информации | Внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями.  Внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы | Использование уязвимостей.  Внедрение вредоносного программного обеспечения.  Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных |

# 7 Актуальные угрозы безопасности информации

В настоящем разделе проведена оценка актуальности угроз безопасности в ИС в соответствии с «Методикой оценки угроз безопасности информации», утвержденной ФСТЭК России 05.02.2021.

В ходе оценки угроз безопасности информации определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей – актуальные угрозы безопасности информации.

## 7.1 Определение возможных угроз безопасности информации

В качестве исходных данных для определения возможных угроз безопасности информации (УБИ) был использован банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Возможные УБИ определяются по результатам оценки возможностей нарушителей, объектов воздействия, возможных способов реализации УБИ и последствий от нарушения свойств безопасности информации.

УБИ возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации УБИ, а реализация угрозы может привести к негативным последствиям:

УБИi = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

В рамках настоящей Модели угроз считается, что нарушителю, обладающему базовыми возможностями (Н1) по реализации УБИ соответствует нарушитель с низким потенциалом, а нарушителю, обладающему базовыми повышенными возможностями (Н2) или средними возможностями (Н3) по реализации УБИ соответствует нарушитель со средним потенциалом в соответствии с банком данных угроз безопасности информации ФСТЭК России.

## 7.2 Сценарии реализации и выводы об актуальности угроз

Сценарии реализации УБИ должны быть определены для соответствующих способов реализации УБИ и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации УБИ.

Перечень основных тактик (тактических задач) и соответствующих им типовых техник, используемых для построения сценариев реализации УБИ в ИС, приведен в Приложении 11 к «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России от 05.02.2021.

В таблице 13 представлены предположения о возможных сценариях реализации угроз применительно к возможным УБИ.

## 7.3 Вывод об актуальности угроз

Угроза безопасности информации признается актуальной при наличии хотя бы одного сценария её реализации. Для каждой угрозы, представленной в таблице 13, присутствует хотя бы один сценарий реализации. Следовательно, угрозы безопасности информации, представленные в таблице 13, являются для ИС актуальными.

Таблица 13 – Перечень актуальных угроз безопасности информации

| **№**  **п/п** | **УБИ** | **Наименование УБИ** | **Негативные последствия** | | |
| --- | --- | --- | --- | --- | --- |
| **К** | **Ц** | **Д** |
|  | 6 | Угроза внедрения кода или данных | 1 | 1 | 1 |
|  | 12 | Угроза деструктивного изменения конфигурации/среды окружения программ | 1 | 1 | 1 |
|  | 25 | Угроза изменения системных и глобальных переменных | 1 | 1 | 1 |
|  | 30 | Угроза использования информации идентификации/аутентификации, заданной по умолчанию | 1 | 1 | 1 |
|  | 63 | Угроза некорректного использования функционала программного обеспечения | 1 | 1 | 1 |
|  | 71 | Угроза несанкционированного восстановления удалённой защищаемой информации | 1 | 0 | 0 |
|  | 86 | Угроза несанкционированного изменения аутентификационной информации | 0 | 1 | 1 |
|  | 89 | Угроза несанкционированного редактирования реестра | 1 | 1 | 1 |
|  | 90 | Угроза несанкционированного создания учётной записи пользователя | 1 | 1 | 1 |
|  | 93 | Угроза несанкционированного управления буфером | 1 | 1 | 1 |
|  | 100 | Угроза обхода некорректно настроенных механизмов аутентификации | 1 | 1 | 1 |
|  | 122 | Угроза повышения привилегий | 1 | 1 | 1 |
|  | 152 | Угроза удаления аутентификационной информации | 1 | 1 | 1 |
|  | 178 | Угроза несанкционированного использования системных и сетевых утилит | 1 | 1 | 1 |
|  | 185 | Угроза несанкционированного изменения параметров настройки средств защиты информации | 1 | 1 | 1 |
|  | 186 | Угроза внедрения вредоносного кода через рекламу, сервисы и контент | 0 | 1 | 1 |
|  | 187 | Угроза несанкционированного воздействия на средство защиты информации | 1 | 1 | 1 |
|  | 188 | Угроза подмены программного обеспечения | 1 | 1 | 1 |
|  | 189 | Угроза маскирования действий вредоносного кода | 0 | 1 | 1 |
|  | 190 | Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет | 1 | 1 | 1 |
|  | 191 | Угроза внедрения вредоносного кода в дистрибутив программного обеспечения | 1 | 1 | 1 |
|  | 192 | Угроза использования уязвимых версий программного обеспечения | 1 | 1 | 1 |

# Заключение

В ходе разработки Модели угроз было осуществлено описание ИС, возможных негативных последствий от реализации угроз, нарушителей информационной безопасности как источников угроз безопасности, а также предположений об их возможностях, которые могут использоваться для разработки и проведения атак, и ограничениях этих возможностей, были определены объекты защиты ИС. На основании перечня источников угроз был определен перечень возможных угроз безопасности информации.

В соответствии с «Методикой оценки угроз безопасности информации» (утверждена ФСТЭК России 5 февраля 2021 г.) проведена оценка возможных сценариев реализации угроз и оценка актуальности угроз. По результатам оценки выявлено 22 актуальные угрозы.

Для обеспечения требований законодательства Российской Федерации, методических и руководящих документов ФСТЭК России должны быть реализованы организационные и технические меры по противодействию актуальным угрозам безопасности информации.

Разработал:

|  |  |  |
| --- | --- | --- |
| Заместитель руководителя отдела исполнения проектов по ИБ ООО «ОРГАН ПО АТТЕСТАЦИИ» | \_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |  |

1. Для повышения уровня своих возможностей нарушители вида 3, 4, 5, 13 могут вступать в сговор с нарушителями 10, 11, 12 видов. [↑](#footnote-ref-2)
2. При сговоре с лицами, обеспечивающими функционирования систем и сетей или обеспечивающими системы оператора, авторизованными пользователями систем, системными администраторами и администраторами безопасности [↑](#footnote-ref-3)