УТВЕРЖДАЮ
Генеральный директор

И.И. Иванов

«___» 2009 г.

М.П.

Модель угроз информационной системы персональных данных "АВТОКАДРЫ"

2009 г.

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АВС	- антивирусные средства
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
АСЗИ	- автоматизированная система в защищенном исполнении
ИСПДн	- информационная система персональных данных
ЛВС	- локальная вычислительная сеть
МЭ	- межсетевой экран
ОС	- операционная система
ПДн	- персональные данные
ПМВ	- программно-математическое воздействие
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
САЗ	- система анализа защищенности
СЗИ	- средства защиты информации
СЗПДн	- система (подсистема) защиты персональных данных
СКЗИ	- средства криптографической защиты информации
СОВ	- система обнаружения вторжений
ТС	- техническое средство
УБПДн	- угрозы безопасности персональных данных

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.

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 объекта – состояние защищенности объекта от внешних и внутренних 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.

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

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

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.

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.

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 – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – это 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 таки 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 способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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.

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.

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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.

Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

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, 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.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Примечание

Так как по своей природе сведения, составляющие государственную тайну, не отличаются от всех остальных сведений, то приведенное определение можно корректно использовать для любых сведений.

Учитывая определение понятия «информация», термин «носитель информации» можно использовать в качестве синонима термину «носитель сведений».

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 невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.).

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.

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

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

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

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

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

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

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

Технические средства информационной системы персональных данных – технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), 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 оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

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 которого невозможно восстановить содержание персональных данных в информационной системе

персональных данных или в результате которых уничтожаются материальные носители 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 - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней 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 - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами в области защиты персональных данных:

[1] - Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] - Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[3] - Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановления Правительства Российской Федерации от 17 ноября 2007 года № 781;

[4] - Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462);

[5] - Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (утверждены 15 февраля 2008г. заместителем директора ФСТЭК России);

[6] - Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

[7] - Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

[8] - Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России).

ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России ([5]-[8]), регламентирующих порядок обеспечения безопасности ПДн.

Настоящая «Модель угроз информационной системы персональных данных "АВТОКАДРЫ"» (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн, связанным:

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

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

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана на основе [5] и [6] с использованием [7] для конкретной ИСПДн "АВТОКАДРЫ" с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль за обеспечением уровня защищенности персональных данных.

В Модели угроз дано обобщённое описание ИСПДн как объекта защиты, возможных источников УБПДн, основных классов уязвимостей ИСПДн, возможных видов неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модели угроз осуществляется также в случае внесения новых элементов в [10]. Кроме того, Модель угроз может быть пересмотрена по решению оператора (Общество с ограниченной ответственностью "ФИРМА") на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование ИСПДн

Наименование ИСПДн – "АВТОКАДРЫ". ИСПДн является собственностью общества с ограниченной ответственностью "ФИРМА".

Местонахождение ИСПДн

ИСПДн располагается по адресу: 624600, Свердловская область, город Екатеринбург, ул. Ленина, 15, ИСПДн занимает помещения №123, №456.

Охрана помещений

Охраной помещений организации занимается предприятие "Охрана", также данное предприятие занимается обслуживанием установленной пожарно-охранной сигнализации.

Взаимодействие с другими ИСПДн

Взаимодействие ИСПДн "АВТОКАДРЫ" с другими информационными системами не предполагается.

ПРИНЦИПЫ МОДЕЛИ УГРОЗ

В основе Модели угроз лежат следующие общие принципы:

1) Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных.

2) При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий.

5) Нарушитель может действовать на различных этапах жизненного цикла ИСПДн.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящий раздел составлен в соответствии с [6] и [7]. В разделе определяются актуальные угрозы безопасности персональных данных, не затрагивающие вопросы, связанные с применением в ИСПДн криптосредств.

Исходные данные

а) Категория обрабатываемых ПДн – Хпд.

В ИСПДн обрабатываются персональные данные, которые позволяют идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением 1 категории персональных данных.

Устанавливается параметр Хпд = категория 2.

б) Объем обрабатываемых ПДн – Хнпд.

В ИСПДн одновременно обрабатываются персональные данные от 1000 до 100000 субъектов персональных данных.

в) Заданные характеристики безопасности ПДн.

Устанавливаются следующие характеристики безопасности ПДн:

№ п/п	Характеристика безопасности	Наличие характеристики безопасности
1	Конфиденциальность	Да
2	Целостность	Нет
3	Доступность	Нет

г) Структура ИСПДн.

По структуре ИСПДн представляет собой локальную информационную систему - комплекс АРМ, объединенных без использования технологии удаленного доступа.

д) Наличие подключений к сетям общего пользования.

Подключение информационной системы к сетям - отсутствует.

е) Режим обработки ПДн.

В ИСПДн режим обработки ПДн многопользовательский с равными правами доступа пользователей.

ж) Местонахождение технических средств ИСПДн.

Местонахождение технических средств информационной системы - все средства находятся в пределах Российской Федерации.

з) Класс ИСПДн.

ИСПДн устанавливается класс К2 - информационная система, для которой нарушение заданной характеристики безопасности персональных данных, обрабатываемых в ней, может привести к негативным последствиям для субъектов персональных данных. Класс ИСПДн устанавливается соответствующим актом.

Показатель исходной защищенности ИСПДн

Информационная система персональных данных (ИСПДн) "АВТОКАДРЫ" имеет следующие технические и эксплуатационные характеристики:

а) Территориальное размещение ИСПДн - локальная ИСПДн, развернутая в пределах одного здания. Уровень защищенности - высокий.
б) ….
в) ….

Определение исходной степени защищенности:

№ п/п	Значение характеристики (уровень защищенности)	Количество значений	Процент значений не ниже данного уровня
1	Высокий	2	….%
2	Средний	3	…%
3	Низкий	2	-

В соответствии полученными данными устанавливается **средний показатель исходной защищенности**. Устанавливается значение коэффициента …**=5**.

Опасность угроз

Для ИСПДн в пункте з) подраздела «Исходные данные» установлен класс ИСПДн К2. Характеристики безопасности информации и объектов ИСПДн заданы в пункте в) подраздела «Исходные данные». Согласно документу [8] класс К2 определяется следующим образом: ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Согласно документу [6] угроза имеет среднюю опасность, если реализация угрозы может привести к негативным последствиям для субъектов персональных данных.

Общее определение угрозы безопасности объекта – возможное нарушение характеристики безопасности объекта.

Определение 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.

Согласно данным положениям для всех угроз частной модели принимается **средняя опасность**.

Источники угроз, связанных с несанкционированным доступом

В таблице приведены наименования, условные обозначения, характеристики источников угроз, связанных с несанкционированным доступом. В таблице приведен полный перечень источников угроз в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный источник угроз существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный источник угроз не может являться источником угроз для рассматриваемой системы в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по нейтрализации данного источника угроз. В столбце «Меры» стоит знак «-», если не приняты меры по нейтрализации данного источника угроз. При оценке актуальности угроз рассматриваются только те источники, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Источник угрозы	Характеристика	Меры приняты	Применимость
1	ИНСД0	Внешний нарушитель	Нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.	-	+

№ п/п	Обозначение	Источник угрозы	Характеристика	Меры приняты	Применимость
			Внешними нарушителями могут быть: - разведывательные службы государств; - криминальные структуры; - конкуренты (конкурирующие организации); - недобросовестные партнеры; - внешние субъекты (физические лица). Внешний нарушитель имеет следующие возможности: к ИСПДн. … …		
2	ИНСД1	Лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступ к ИР	К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн. Лицо этой категории, может: - иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; - располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; - располагать именами и вести выявление паролей зарегистрированных пользователей; - изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и	-	+

№ п/п	Обозначение	Источник угрозы	Характеристика	Меры приняты	Применимость
			обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.		
…	…	…	…	…	…
23	ИНСД22	Макро-вирусы	…	+	-

Разные источники могут приводить к реализации схожих угроз, связанных с несанкционированным доступом. В результате анализа характеристик источников угроз и особенностей функционирования ИСПДн, источники угроз сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Источники НСД 1"	ИНСД0
2	Список "Источники НСД 2"	ИНСД0, ИНСД2, ИНСД3, ИНСД4, ИНСД5, ИНСД6
3	Список "Источники НСД 3"	ИНСД2, ИНСД3, ИНСД4, ИНСД5, ИНСД6
4	Список "Источники НСД 4"	ИНСД2, ИНСД3, ИНСД4, ИНСД5, ИНСД6, ИНСД9
5	Список "Источники НСД 5"	ИНСД7, ИНСД8
6	Список "Источники НСД 6"	ИНСД7, ИНСД8, ИНСД9
7	Список "Источники НСД 7"	ИНСД9
8	Список "Источники НСД 8"	ИНСД10, ИНСД11
9	Список "Источники НСД 9"	ИНСД12, ИНСД13, ИНСД14
10	Список "Источники НСД 10"	ИНСД15
11	Список "Источники НСД 11"	ИНСД16, ИНСД17, ИНСД18, ИНСД19, ИНСД20, ИНСД21

Уязвимости ИСПДн

В таблице приведены наименования, условные обозначения, характеристики возможных уязвимостей ИСПДн, связанных с несанкционированным доступом. В таблице приведен полный перечень уязвимостей в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данная уязвимость существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данная уязвимость не может привести к реализации угрозы для рассматриваемой системы в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по устранению данной уязвимости. В столбце «Меры» стоит знак «-», если не приняты меры по устранению данной уязвимости. При оценке актуальности угроз рассматриваются только те уязвимости, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Уязвимость	Характеристика	Меры приняты	Применимость
1	У0	Уязвимости микропрограмм, прошивок ПЗУ, ППЗУ (наличие в ИСПДн вредоносной программы)	Уязвимости в микропрограммах могут представлять собой: - фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации,	+	+

№ п/п	Обозначение	Уязвимость	Характеристика	Меры приняты	Применимость
			аутентификации, проверки целостности и др.; … …		
2	У1	Уязвимости драйверов аппаратных средств (наличие в ИСПДн вредоносной программы)		+	+
…	…	…	…	…	…
18	У17	Уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе и отказов этих средств		-	+

Разные уязвимости могут приводить к реализации схожих угроз, связанных с несанкционированным доступом. В результате анализа характеристик уязвимостей и особенностей функционирования ИСПДн, уязвимости сгруппированы в списки, которые представлены в таблице. Уязвимости, входящие в один и тот же список, могут быть использованы для реализации схожих угроз.

№ п/п	Название списка	Элементы списка
1	Список "Уязвимости 1"	У0, У1, У2, У3, У4
2	Список "Уязвимости 2"	У0, У1, У2, У3, У4, У5, У6, У7
3	Список "Уязвимости 3"	У2, У3, У4, У5, У6, У7
4	Список "Уязвимости 4"	У8
5	Список "Уязвимости 5"	У9, У10, У11, У12, У13, У14
6	Список "Уязвимости 6"	У15
7	Список "Уязвимости 7"	У15, У16, У17
8	Список "Уязвимости 8"	У16, У17

Способы реализации угроз

В таблице приведены наименования, условные обозначения, характеристики способов реализации угроз, связанных с несанкционированным доступом. В таблице приведен полный перечень способов реализации угроз в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный способ реализации угроз существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный способ реализации угроз не может привести к реализации угроз для рассматриваемой системы в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по устранению данного способа реализации угроз. В столбце «Меры» стоит знак «-», если не приняты меры по устранению данного способа реализации угроз. При оценке актуальности угроз рассматриваются только те способы реализации угроз, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Способ реализации	Характеристика	Меры приняты	Применимость

№ п/п	Обозначение	Способ реализации	Характеристика	Меры приняты	Применимость
1	P0	Обход СЗИ используя существующие уязвимости программно-аппаратного обеспечения ИСПДн		-	+
…	…	…	…	…	…
41	P40	Нетрадиционные информационные каналы	В нетрадиционных информационных каналах, основанных на манипуляции различных характеристик ресурсов ИСПДн, используются для передачи данных некоторые разделяемые ресурсы. сформированы на различных уровнях функционирования ИСПДн: - на аппаратном уровне; - на уровне микрокодов и драйверов устройств; - на уровне операционной системы; - на уровне прикладного программного обеспечения; - на уровне функционирования каналов передачи данных и линий связи. ….	-	+

Разные способы реализации могут быть использованы для реализации схожих угроз, связанных с несанкционированным доступом. В результате анализа характеристик способов реализации и особенностей функционирования ИСПДн, способы реализации сгруппированы в списки, которые представлены в таблице. Способы реализации, входящие в один и тот же список, могут быть использованы для реализации схожих угроз.

№ п/п	Название списка	Элементы списка
1	Список "Реализации 1"	P0, P1, P2
2	Список "Реализации 2"	P0, P1, P2, P3, P4, P5, P6, P7, P11, P13, P14
3	Список "Реализации 3"	P0, P1, P2, P3, P4, P5, P6, P7, P11, P13, P14, P15
4	Список "Реализации 4"	P0, P1, P2, P9
5	Список "Реализации 5"	P0, P1, P2, P9, P10, P11, P17
6	Список "Реализации 6"	P0, P1, P2, P9, P11

№ п/п	Название списка	Элементы списка
7	Список "Реализации 7"	P0, P1, P2, P9, P11, P19, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29, P30, P31, P32, P33, P34, P35, P36, P37, P38, P39, P40
8	Список "Реализации 8"	P0, P1, P2, P10, P11, P17
9	Список "Реализации 9"	P0, P1, P2, P10, P11, P17, P18
10	Список "Реализации 10"	P0, P1, P2, P11
11	Список "Реализации 11"	P0, P1, P2, P11, P18
12	Список "Реализации 12"	P0, P1, P2, P18
13	Список "Реализации 13"	P3, P4, P5, P6, P7, P13, P14
14	Список "Реализации 14"	P3, P4, P5, P6, P7, P13, P14, P15
15	Список "Реализации 15"	P8, P9, P16, P19, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29, P30, P31, P32, P33, P34, P35, P36, P37, P38, P39, P40
16	Список "Реализации 16"	P8, P16
17	Список "Реализации 17"	P9, P19, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29, P30, P31, P32, P33, P34, P35, P36, P37, P38, P39, P40
18	Список "Реализации 18"	P18
19	Список "Реализации 19"	P18, P19, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29, P30, P31, P32, P33, P34, P35, P36, P37, P38, P39, P40
20	Список "Реализации 20"	P19, P20, P21, P22, P23, P24, P25, P26, P27, P28, P29, P30, P31, P32, P33, P34, P35, P36, P37, P38, P39, P40

Объекты воздействия

В таблице приведены наименования, условные обозначения, характеристики объектов воздействия угроз, связанных с несанкционированным доступом. В таблице приведен полный перечень объектов воздействия в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный объект воздействия существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный объект воздействия отсутствует и не может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по защите данного объекта воздействия. В столбце «Меры» стоит знак «-», если не приняты меры по защите данного объекта воздействия. При оценке актуальности угроз рассматриваются только те объекты воздействия, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Объект воздействия	Характеристика	Меры приняты	Применимость
1	O0	Информация, обрабатываемая на АРМ (узле) вычислительной сети на гибких магнитных дисках		-	-
…	…	…	…	…	…
32	O31	Информация на прикладном уровне		+	+

Разные объекты воздействия могут быть подвержены схожим угрозам, связанным с несанкционированным доступом. В результате анализа характеристик объектов воздействия и особенностей функционирования ИСПДн, объекты воздействия сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Объекты 1"	O1, O3, O8, O9, O10, O11
2	Список "Объекты 2"	O1, O3, O8, O9, O10, O11, O12, O13, O14, O15, O19, O23, O24, O25
3	Список "Объекты 3"	O1, O3, O8, O9, O10, O11, O12, O13, O14, O15, O19, O23, O24, O25, O26, O27, O28, O29, O30, O31

№ п/п	Название списка	Элементы списка
4	Список "Объекты 4"	О1, О3, О8, О9, О10, О11, О26, О27, О28, О29, О30, О31
5	Список "Объекты 5"	О12, О13, О14, О15, О19, О23, О24, О25
6	Список "Объекты 6"	О26, О27, О28, О29, О30, О31

Деструктивные действия

В таблице приведены наименования, условные обозначения, характеристики деструктивных действий, связанных с несанкционированным доступом. В таблице приведен полный перечень деструктивных действий в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данное деструктивное действие может быть осуществлено в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данное деструктивное действие не может быть осуществлено в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по защите от данного деструктивного действия. В столбце «Меры» стоит знак «-», если не приняты меры по защите от данного деструктивного действия. При оценке актуальности угроз рассматриваются только те деструктивные действия, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Деструктивное действие	Характеристика	Меры приняты	Применимость
1	Д0	Утечка информации обрабатываемой на объекте		-	+
…	…	…	…	…	…
31	Д30	Нарушение и отказы функционирования СЗИ		+	+

Разные деструктивные действия могут быть результатом реализации схожих угроз, связанных с несанкционированным доступом. В результате анализа характеристик деструктивных действий и особенностей функционирования ИСПДн, деструктивные действия сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Действия 1"	Д0, Д1, Д2, Д3, Д4, Д5, Д6, Д7, Д8, Д9, Д10, Д11
2	Список "Действия 2"	Д0, Д1, Д2, Д3, Д4, Д5, Д6, Д7, Д8, Д9, Д10, Д11, Д12, Д13, Д14, Д15, Д16, Д17, Д18, Д19, Д20, Д21, Д22, Д23, Д24, Д25, Д26, Д27, Д28, Д29, Д30
3	Список "Действия 3"	Д12, Д13, Д14, Д15, Д16, Д17, Д18, Д19, Д20, Д21, Д22, Д23, Д24, Д25, Д26, Д27, Д28, Д29, Д30

Источники угроз, связанных с техническими каналами утечки

В таблице приведены наименования, условные обозначения, характеристики источников угроз, связанных с утечкой по техническим каналам. В таблице приведен полный перечень источников угроз в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный источник угроз существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный источник угроз не может являться источником угроз для рассматриваемой системы в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по нейтрализации данного источника угроз. В столбце «Меры» стоит знак «-», если не приняты меры по нейтрализации данного источника угроз. При оценке

актуальности угроз рассматриваются только те источники, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Источник угрозы	Характеристика	Меры приняты	Применимость
1	ИТКУИ0	Физические лица, не имеющие доступа к ИСПД		-	+
2	ИТКУИ1	Зарубежные спец службы		-	-
3	ИТКУИ2	Зарубежные организации		-	+
4	ИТКУИ3	Криминальные группировки		-	+

Разные источники могут приводить к реализации схожих угроз, связанных с утечкой по техническим каналам. В результате анализа характеристик источников угроз и особенностей функционирования ИСПДн, источники угроз сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Источники ТКУИ 1"	ИТКУИ0, ИТКУИ2, ИТКУИ3

Носители ПДн

В таблице приведены наименования, условные обозначения, характеристики носителей ПДн. В таблице приведен полный перечень носителей ПДн в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный носитель ПДн существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный носитель ПДн не существует и не может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по защите данного носителя ПДн. В столбце «Меры» стоит знак «-», если не приняты меры по защите данного носителя ПДн. При оценке актуальности угроз рассматриваются только те носители ПДн, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Носитель ПДн	Характеристика	Меры приняты	Применимость
1	Н0	Пользователь ИСПД, осуществляющий голосовой ввод ПД		-	-
2	Н1	Акустическая система ИСПД воспроизводящая ПД		-	-
3	Н2	ВТСС и ТС ИСПД создающие физические поля, в которых информация находит свое отражение		-	+

Разные носители ПДн могут быть объектом схожих угроз, связанных с утечкой по техническим каналам. В результате анализа характеристик носителей ПДн и особенностей функционирования ИСПДн, носители ПДн сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Носители ПД 1"	H2

Технические каналы утечки

В таблице приведены наименования, условные обозначения, характеристики технических каналов утечки информации. В таблице приведен полный перечень технических каналов в соответствии с [7]. В столбце «Применимость» стоит знак «+», если данный канал утечки существует или может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Применимость» стоит знак «-», если данный канал утечки не существует и не может появиться в рассматриваемой системе в связи с особенностями технологического процесса обработки информации. В столбце «Меры» стоит знак «+», если приняты меры по устранению данного канала утечки. В столбце «Меры» стоит знак «-», если не приняты меры по устранению данного канала утечки. При оценке актуальности угроз рассматриваются только те каналы утечки, у которых в столбце «Применимость» стоит знак «+».

№ п/п	Обозначение	Канал утечки	Характеристика	Меры приняты	Применимость
1	K0	Акустооптика	Оптические излучения, …	-	-
15	K14	Волоконно-оптическая система передачи данных	Для волоконно-оптической системы передачи данных угрозой утечки информации является… … …	-	-

Разные источники могут приводить к реализации схожих угроз, связанных с утечкой по техническим каналам. В результате анализа характеристик источников угроз и особенностей функционирования ИСПДн, источники угроз сгруппированы в списки, которые представлены в таблице.

№ п/п	Название списка	Элементы списка
1	Список "Каналы утечки 1"	K7, K8, K9
2	Список "Каналы утечки 2"	K10, K11, K12, K13

Списки актуальных угроз

Угрозы скомпонованы в множества для краткости представления. Каждая угроза, связанная с несанкционированным доступом, представлена в виде упорядоченной пятерки: <источник угрозы, уязвимость, способ реализации, объект воздействия, деструктивное действие>. Каждая угроза, связанная с утечкой информации по техническим каналам, представлена в виде упорядоченной тройки <источник угрозы, носитель ПДн, канал утечки>. По результатам обследования ИСПДн определено наличие мер и предпосылок для возможных угроз.

Меры для нейтрализации угрозы считаются принятыми и достаточными, если они позволяют нейтрализовать все компоненты угрозы. Меры считаются принятыми, но недостаточными, если нейтрализуются не все компоненты угрозы. Меры считаются не принятыми, если они не позволяют нейтрализовать ни один компонент угрозы. Решение о наличии мер для нейтрализации каждой угрозы принимается на основе обследования ИСПДн.

Существование предпосылок для угроз определяется экспертом с учетом особенностей архитектуры и функционирования ИСПДн.

Вероятность угрозы определяется по таблице:

	Меры не приняты	Меры недостаточны	Меры достаточны
Есть предпосылки	Высокая вероятность	Средняя вероятность	Низкая вероятность
Нет предпосылок	Маловероятно	Маловероятно	Маловероятно

По вероятности для угрозы определяется коэффициент $Y_{...}$.

Далее, для каждой угрозы в зависимости от вероятности и исходного уровня защищенности определяется возможность ее реализации – коэффициент Y = …..

Опасность угроз зависит от класса ИСПДн и уже установлена в начале раздела. Актуальность угроз определяется по возможности и опасности угрозы. В таблице представлены только актуальные угрозы.

№ п/п	Множество угроз	Предпосылки	Меры	…	Коэфициент вероятности	Вероятность	…	Возможность	Опасность	Актуальность
1	< ИНСД0, Уязвимости 7, Реализации 7, Объекты 1, Действия 1 >	Есть	Не приняты	5	10	Высокая	0,75	Высокая	Средняя	Да
…	…	…	…	…	…	…	…	…	…	…
32	< Источники НСД 5, У15, Реализации 9, Объекты 6, Действия 2 >	Есть	Недостаточны	5	5	Средняя	0,50	Средняя	Средняя	Да
33	< Источники НСД 6, У15, Реализации 14, Объекты 3, Действия 2 >	Есть	Недостаточны	5	5	Средняя	0,50	Средняя	Средняя	Да
…	…	…	…	…	….					
63	< Источники ТКУИ 1, Н2, Каналы утечки 1 >	Есть	Недостаточны	5	5	Средняя	0,50	Средняя	Средняя	Да

Экспертная комиссия:

Председатель комиссии _____ _____

Члены комиссии

_____ _____

_____ _____

_____ _____