**Базовая модель  
угроз безопасности персональных данных при их обработке в информационных системах персональных данных  
(выписка)  
(утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.)**

Обозначения и сокращения

**АРМ** - автоматизированное рабочее место

**ВИ** - видовая информация

**ВТСС** -  вспомогательные технические средства и системы

**ИСПДн** - информационная система персональных данных

**КЗ** - контролируемая зона

**МЭ** - межсетевой экран

**НДВ** - недекларированные возможности

**НСД** - несанкционированный доступ

**ОБПДн** - обеспечение безопасности персональных данных

**ОС** - операционная система

**ПДн** - персональные данные

**ПМВ** - программно-математическое воздействие

**ПО** - программное обеспечение

**ПЭМИН** - побочные электромагнитные излучения и наводки

**РИ** - речевая информация

**СВТ** - средство вычислительной техники

**СЗИ** - средство защиты информации

**СПИ** - стеганографическое преобразование информации

**СЭУПИ** - специальные электронные устройства перехвата информации

**ТКУИ** - технический канал утечки информации

**ТСОИ** - технические средства обработки информации

**УБПДн** - угрозы безопасности персональных данных

**1. Термины и определения**

В настоящем документе используются следующие термины и их определения:

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

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

**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.

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

**Доступ к информации** - возможность получения информации и ее использования.

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

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

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

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**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 таких средств.

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

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

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

**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.

**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.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

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

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

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

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

**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.

**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, 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.

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

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

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

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

**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** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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.

**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.

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

**Уязвимость** - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

**2. Общие положения**

Настоящая "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (далее - Модель угроз) содержит систематизированный перечень угроз [**безопасности персональных данных**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_13) при их обработке в [**информационных системах персональных данных**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_24). Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных ([**ПДн**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7711)), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных ([**ИСПДн**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_774)), связанным:

с [**перехватом**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_36) (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 государственных и муниципальных органов, юридических и (или) физических лиц (далее - [**операторов**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_35)), организующих и (или) осуществляющих обработку ПДн, а также определяющих цели и содержание обработки ПДн, заказчиков и разработчиков ИСПДн и их подсистем. С применением Модели угроз решаются следующие задачи:

разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

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**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_32) 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 обеспечения уровня защищенности персональных данных.

В Модели угроз дано обобщенное описание ИСПДн как объектов защиты, возможных [**источников угрозы безопасности персональных данных**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_26) ([**УБПДн**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7722)), основных классов уязвимостей ИСПДн, возможных видов 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 Модель угроз осуществляется ФСТЭК России в устанавливаемом порядке.

**3. Классификация угроз безопасности персональных данных**

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения [**информативных сигналов**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_23), содержащих [**защищаемую информацию**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_21), и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы [**обработки персональных данных**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_34), режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также [**информационных технологий**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_25), применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

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) (далее - технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.);

средства защиты информации;

[**вспомогательные технические средства и системы**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_17) ([**ВТСС**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_773)) - технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее - служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн ([**рисунок 1**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7701)) являются:

источник УБПДн - субъект, материальный объект или физическое явление, создающие УБПДн;

среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

┌──────────────────┐    ┌────────────────────────┐    ┌─────────────────┐

│                  │    │ Среда распространения  │    │                 │

│      Источник    │    │   ПДн и воздействий    │    │                 │

│угроз безопасности├◄──►┤       Приемник         ├◄──►│  Наситель ПДн   │

│      ПДн         │    │ информативного сигнала │    │                 │

│                  │    │       Передатчик       │    │                 │

└──────────────────┘    │воздействующего сигнала │    └─────────────────┘

                        └────────────────────────┘

**Рисунок 1. Обобщенная схема канала реализации угроз безопасности персональных данных**

Носители ПДн могут содержать информацию, представленную в следующих видах:

акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками ([**рисунок 2**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7702)):

по виду защищаемой от УБПДн информации, содержащей ПДн;

по видам возможных источников УБПДн;

по типу ИСПДн, на которые направлена реализация УБПДн;

по способу реализации УБПДн;

по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

по используемой уязвимости;

по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и [**вредоносных программ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_16).

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места ([**АРМ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_771));

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

"Рисунок 2. Классификация угроз безопасности персональных данных"

Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

угрозы, связанные с [**НСД**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_778) к ПДн (в том числе угрозы внедрения вредоносных программ);

угрозы утечки ПДн по [**техническим каналам утечки информации**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_47);

угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

угрозы, реализуемые с использованием уязвимости системного [**ПО**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7713);

угрозы, реализуемые с использованием уязвимости прикладного ПО;

угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

угрозы, реализуемые с использованием уязвимостей [**СЗИ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7717).

По объекту воздействия выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых на АРМ;

угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

угрозы безопасности ПДн, передаваемых по сетям связи;

угрозы прикладным программам, с помощью которых обрабатываются ПДн;

угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДн:

значительным негативным последствиям для субъектов ПДн;

негативным последствиям для субъектов ПДн;

незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД) (далее - угрозы НСД в ИСПДн), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <[**уязвимость**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_51) программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

**4. Угрозы утечки информации по техническим каналам**

Основными элементами описания угроз утечки информации по техническим каналам ([**ТКУИ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7720)) являются: источник угрозы, среда (путь) распространения информативного сигнала и носитель защищаемой информации.

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИСПДн, а также зарубежные спецслужбы или организации (в том числе конкурирующие или террористические), криминальные группировки, осуществляющие перехват (съем) информации с использованием технических средств ее регистрации, приема или фотографирования.

Среда распространения информативного сигнала - это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником. Среда распространения может быть как однородной (например, только воздушной), так и неоднородной за счет перехода сигнала из одной среды в другую (например, в результате акустоэлектрических или виброакустических преобразований).

Носителем ПДн является пользователь ИСПДн, осуществляющий голосовой ввод ПДн в ИСПДн, акустическая система ИСПДн, воспроизводящая ПДн, а также технические средства ИСПДн и ВТСС, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

При обработке ПДн в ИСПДн за счет реализации технических каналов утечки информации возможно возникновение следующих УБПДн:

угроз утечки акустической (речевой) информации;

угроз утечки видовой информации;

угроз утечки информации по каналам [**побочных электромагнитных излучений и наводок**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_38) ([**ПЭМИН**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7714)).

**4.1. Угрозы утечки акустической (речевой) информации**

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Перехват акустической (речевой) информации в данных случаях возможен с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки ПДн, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн.

Кроме этого, перехват акустической (речевой) информации возможен с использованием специальных электронных устройств съема речевой информации, внедренных в технические средства обработки ПДн, ВТСС и помещения или подключенных к каналам связи.

Угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации ("[**закладочных устройств**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_20)"), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Перехват акустической (речевой) информации может вестись:

стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

портативной носимой аппаратурой - физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них;

автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами непосредственно в служебных помещениях или в непосредственной близости от них.

**4.2. Угрозы утечки видовой информации**

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Угрозы безопасности ПДн, связанные с их перехватом при использовании специальных электронных устройств съема видовой информации (видеозакладок), определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Перехват ПДн может вестись:

стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

портативной возимой аппаратурой, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

портативной носимой аппаратурой - физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них.

Перехват (просмотр) ПДн может осуществляться посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо с расстояния прямой видимости из-за пределов ИСПДн с использованием оптических (оптикоэлектронных) средств.

**4.3. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок**

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, обрабатывающих ПДн (в средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, в том числе в средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео- и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПДн.

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;

портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;

портативной носимой аппаратурой - физическими лицами в непосредственной близости от ИСПДн;

автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от ИСПДн.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий технических средств ИСПДн и ВТСС и посторонних проводников (в том числе цепей электропитания и заземления).

Наводки электромагнитных излучений технических средств ИСПДн возникают при излучении элементами технических средств ИСПДн информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПДн, линий ВТСС и посторонних проводников. В результате на случайных антеннах (цепях ВТСС или посторонних проводниках) наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связи источника информативных сигналов в составе технических средств ИСПДн и цепей питания.

Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связи источника информативных сигналов в составе аппаратуры ТСПИ и цепей заземления.

Для съема информации с проводных линий могут использоваться:

средства съема сигналов, содержащих защищаемую информацию, с цепей технических средств ИСПДн и ВТСС, линий связи и передачи данных, выходящих за пределы служебных помещений (эквиваленты сети, токовые трансформаторы, пробники);

средства съема наведенных информативных сигналов с цепей электропитания;

средства съема наведенных информативных сигналов с шин заземления;

средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

Для волоконно-оптической системы передачи данных угрозой утечки информации является утечка оптического излучения, содержащего защищаемую информацию, с боковой поверхности оптического волокна.

Появление новых каналов связи - сотовой связи, пейджинговых сообщений, спутниковых и беспроводных сетей передачи данных - привело к развитию специализированных систем и средств контроля и перехвата информации, ориентированных на используемые в них информационные технологии, в том числе средств:

перехвата пейджинговых сообщений и сотовой связи;

перехвата информации в каналах передачи данных вычислительных сетей.

**5. Угрозы несанкционированного доступа к информации в информационной системе персональных данных**

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения);

угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

угрозы внедрения вредоносных программ ([**программно-математического воздействия**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_42)).

Состав элементов описания угроз НСД к информации в ИСПДн приведен на [**рисунке 3**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7703).

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

Угрозы [**доступа (проникновения) в операционную среду**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_18) ИСПДн с использованием штатного программного обеспечения разделяются на угрозы непосредственного и удаленного доступа. Угрозы непосредственного доступа осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера. Угрозы удаленного доступа реализуются с использованием протоколов сетевого взаимодействия.

Эти угрозы реализуются относительно ИСПДн как на базе автоматизированного рабочего места, не включенного в сети связи общего пользования, так и применительно ко всем ИСПДн, имеющим подключение к сетям связи общего пользования и сетям международного информационного обмена.

Описание угроз доступа (проникновения) в операционную среду компьютера формально может быть представлено следующим образом:

угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств - это угрозы "Отказа в обслуживании". Как правило, данные угрозы рассматриваются применительно к ИСПДн на базе локальных и распределенных информационных систем вне зависимости от подключения информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного программного обеспечения не учитывается возможность преднамеренных действий по целенаправленному изменению:

содержания служебной информации в пакетах сообщений, передаваемых по сети;

условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);

форматов представления данных (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

программного обеспечения обработки данных.

В результате реализации угроз "Отказа в обслуживании" происходит переполнение буферов и блокирование процедур обработки, "зацикливание" процедур обработки и "зависание" компьютера, отбрасывание пакетов сообщений и др. Описание таких угроз формально может быть представлено следующим образом:

угроза "Отказа в обслуживании": = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (носитель ПДн)>, <непосредственный результат реализации угрозы (переполнение буфера, блокирование процедуры обработки, "зацикливание" обработки и т.п.)>.

Угрозы внедрения вредоносных программ (программно-математического воздействия) нецелесообразно описывать с той же детальностью, что и вышеуказанные угрозы. Это обусловлено тем, что, во-первых, количество вредоносных программ сегодня уже значительно превышает сто тысяч. Во-вторых, при организации защиты информации на практике, как правило, достаточно лишь знать класс вредоносной программы, способы и последствия от ее внедрения (инфицирования). В связи с этим угрозы программно-математического воздействия ([**ПМВ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_7712)) формально могут быть представлены следующим образом:

угроза ПМВ в ИСПДн: = <класс вредоносной программы (с указанием среды обитания)>, <источник угрозы (носитель вредоносной программы)>, <способ инфицирования>, <объект воздействия (загрузочный сектор, файл и т.п.)>, <описание возможных деструктивных действий>, <дополнительная информация об угрозе (резидентность, скорость распространения, полиморфичность и др.)>.

Ниже дается общая характеристика источников угроз безопасности информации, уязвимостей, которые могут быть использованы при реализации угроз НСД, и характеристика результатов несанкционированного или случайного доступа. Характеристика способов реализации угроз дается при описании угроз доступа (проникновения) в операционную среду компьютера, угроз отказа в обслуживании и угроз ПМВ.

"Рисунок 3. Элементы описания угроз НДС к информации в ИСПДн"

**5.1. Общая характеристика источников угроз несанкционированного доступа в информационной системе персональных данных**

Источниками угроз НСД в ИСПДн могут быть:

нарушитель;

носитель вредоносной программы;

аппаратная закладка.

Угрозы безопасности ПДн, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в [**контролируемую зону**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_27) ([**КЗ**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_775)) ИСПДн нарушители подразделяются на два типа:

нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, - внешние нарушители;

нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, - внутренние нарушители.

Внешними нарушителями могут быть:

разведывательные службы государств;

криминальные структуры;

конкуренты (конкурирующие организации);

недобросовестные партнеры;

внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных [**вирусов**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_15), вредоносных программ, алгоритмических или программных закладок;

осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. 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 обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо этой категории:

обладает всеми возможностями лиц первой категории;

знает, по меньшей мере, одно легальное имя доступа;

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

Его доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими [**правилами разграничения доступа**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_40).

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Лицо этой категории:

обладает всеми возможностями лиц первой и второй категорий;

располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;

имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

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

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн;

обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;

имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД.

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо этой категории:

обладает всеми возможностями лиц предыдущих категорий;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

К седьмой категории относятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

обладает возможностями внесения ошибок, [**недекларированных возможностей**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_31), программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

Лицо этой категории:

обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Указанные категории нарушителей должны учитываться при оценке возможностей реализации УБПДн.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;

встроенные [**носители информации**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_33) (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, - видеоадаптера, сетевой платы, звуковой платы, модема, устройств ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

пакеты передаваемых по компьютерной сети сообщений;

файлы (текстовые, графические, исполняемые и т.д.).

**5.2. Общая характеристика уязвимостей информационной системы персональных данных**

Уязвимость информационной системы персональных данных - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

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

Классификация основных уязвимостей ИСПДн приведена на рисунке  4.

"Рисунок 4. Классификация уязвимостей программного обеспечения"

Ниже представлена общая характеристика основных групп уязвимостей ИСПДн, включающих:

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

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

**5.2.1. Общая характеристика уязвимостей системного программного обеспечения**

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

При этом возможны уязвимости:

в микропрограммах, в прошивках ПЗУ, ППЗУ;

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

в средствах операционной системы, предназначенных для выполнения вспомогательных функций, - утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах (компиляторах, компоновщиках, отладчиках и т.п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т.п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода/вывода и т.д.);

в средствах коммуникационного взаимодействия (сетевых средствах) операционной системы.

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

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

фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры [**идентификации**](http://www.rsoc.ru/admin/_edit2/tinymce/plugins/paste/pasteword.htm#sub_22), аутентификации, проверки целостности и др.;

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

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

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Краткая характеристика этих уязвимостей применительно к протоколам приведена в таблице 2.

**Таблица 2**

**Уязвимости отдельных протоколов стека протоколов TCP/IP, на базе которого функционируют глобальные сети общего пользования**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование протокола | Уровень стека протоколов | Наименование (характеристика) уязвимости | Содержание нарушения безопасности информации |
| FTP (File Transfer Protocol) - протокол передачи файлов по сети | Прикладной, представительный, сеансовый | 1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)  2. Доступ по умолчанию  3. Наличие двух открытых портов | Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей).  Получение удален |