ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ МКОУ СОШ№6г.п.НАРТКАЛА

в отношении обработки персональных данных работников учреждения, обучающихся, воспитанников, родителей (законных представителей)

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 или5 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 при их обработке в информационных системах персональных данных. 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), 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), 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.

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 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 (УБПДн), 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, содержащих защищаемую информацию, 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, 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, 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 (ВТСС) - 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 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.

4. 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*** :
- 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.

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);
- 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);

Классификация угроз безопасност и персональных данных

По виду защищаемой от УБПДн информации, содержащей ПДн

- Угрозы РИ;
- Угрозы ВИ;
- Угрозы информации, обрабатываем ой в ТСОИ;
- Угрозы информации, обрабатываем ой в АС;
- По виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн;
- Угрозы конфиденциальности (утечки, перехвата, съема, копирования, хищения, разглаш ения) информации;
- Угрозы целостности (утраты , уничтож ния, модификации) информации;
- Угрозы доступности (блокирования) инф орм ации По типу ИСПДн, на которые направлена реализация УБПДн;
- Угрозы безопасности ПД н, обрабатываем ы х в ИСПД н на базе АРМ (с подклю чением и без подключения к вычислительной сети).

Классификация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных 1415 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 к ПДн (в том числе угрозы внедрения вредоносных программ); угрозы утечки ПДн по техническим каналам утечки информации;
- 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;
- 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.

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.

5. Угрозы утечки информации по техническим каналам

Основными элементами описания угроз утечки информации по техническим каналам (ТКУИ) 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 (ПЭМИН).

6.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).

Состав элементов описания угроз НСД к информации в ИСПДн приведен на рисунке 3. 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 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.

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.

7.Источник угрозы

- Программно-аппаратная закладка.
- Конструктивно встроенная Автономная Вредоносная программа.
- Программные закладки.
- Программные вирусы.
- Уязвимости ИСПДн.
- Уязвимости ПО Уязвимости прикладного ПО.
- Уязвимости специального ПО.
- Уязвимости ПО пользователя.
- Вредоносные программы, распространяющиеся по сети (черви)
- Другие вредоносные программы.

8. Способ реализации угрозы

Внедрение (внесение) новых уязвимостей в ИСПДн на этапе проектирования, разработки и сопровождения ИСПДн.

- Использование нештатного ПО.
- Объект воздействия Информация, обрабатываемая на АРМ (узле).
- ИСПДн, находящаяся: На отчуждаемых носителях _____ информации_____
- На гибких магнитных дисках
- На жестких магнитных дисках
- На накопителях ZIP На накопителях электронной памяти типа флеш
- На аудио-, видеокассетах, магнитных лентах

- В других устройствах
- На встроенных носителях долговременного хранения информации
- В ПЗУ
- На перепрограммируемых (перезаписываемых) запоминающих устройствах
- В средствах обработки и хранения оперативной информации -|
- В оперативной памяти
- В кеш-памяти, в буферах ввода/вывода –
  В видео-памяти
- В оперативной памяти 1 подключаемых устройств
- Информация в средствах, реализующих сетевое взаимодействие, и каналах передачи данных в сети.