

Рассмотрено
Педагогическим советом
(протокол от 31.08.2018 №11)

Утверждаю
Директор МАОУ «Гимназия города Юрги
Л.Ю. Карпова
31.08.2018



**ЧАСТНАЯ МОДЕЛЬ
УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
Муниципального автономного общеобразовательного учреждения
«Гимназия города Юрги»
в отношении обработки персональных данных сотрудников, а также учащихся и
их законных представителей**

Содержание

Обозначения и сокращения	3
1. Термины и определения.....	4
2. Общие положения.....	8
3. Исходные данные об ИСПДн	10
4. Классификация угроз безопасности персональных данных.....	12
5. Угрозы утечки информации по техническим каналам	17
6. Угрозы несанкционированного доступа к информации в информационной системе персональных данных.....	18
6.1. Общая характеристика источников угроз несанкционированного доступа в информационной системе персональных данных.....	21
6.2. Общая характеристика угроз непосредственного доступа в операционную среду информационной системы персональных данных.....	26
6.3. Общая характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия.....	27
6.4. Общая характеристика угроз программно-математических воздействий	29
6.5. Общая характеристика результатов несанкционированного или случайного доступа.....	36
7. Частная модель угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных.....	38
7.1. Частная модель угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования и (или)сетям международного информационного обмена.....	38
7.2. Частная модель угроз безопасности персональных данных, обрабатываемых в региональных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.....	39
7.3. Вероятность реализации угроз для ИСПДн МАОУ «Гимназия города Юрги».....	40-41

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, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение 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 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, позволяющий 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.

Разработка частной модели угроз безопасности персональных данных в информационной системе персональных данных МАОУ «Гимназия города Юрги» (далее - ИСПДн), проведена в соответствии с требованиями следующих документов:

1. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;
2. Положение об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных (постановление Правительства РФ от 17 ноября 2007 года №781);
3. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России от 14 февраля 2008 года);
4. «Методика определения актуальности угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России от 14 февраля 2008 года);
5. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»;
6. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;
7. Положение о методах и способах защиты информации в информационных системах персональных данных (Приказ ФСТЭК России от 18 февраля 2013г. № 21).

Настоящая Модель угроз безопасности 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 (далее - 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:

- 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 (далее - 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. Исходные данные об ИСПДн

Назначение и состав

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).

ИСПДн 1 - предназначена для хранения и сбора ПДн учащихся, а именно Ф.И.О., даты рождения, пола, серии документа, типа документа, маски участия в ОГЭ и ЕГЭ, МАОУ «Гимназия города Юрги», класса, должности, данные о сдаче экзамена. В состав ИСПДн входят: технические средства и их программное обеспечение, информационные ресурсы, периферийное оборудование.

ИСДн 2 - Электронная школа 2.0, позволяющая автоматизировать деятельность МАОУ «Гимназия города Юрги» и интегрировать государственные и муниципальные услуги в сфере образования с единым порталом государственных услуг (ЕПГУ).

ИСДн 3 – АИС «Образование», совокупность программно-аппаратных средств, предназначенных для автоматизации деятельности, связанной с хранением, передачей и обработкой информации.

Условия размещения и особенности функционирования ИСПДн

ИСПДн 1 является автоматизированным рабочим местом. Технические средства ИСПДн размещены в помещении, находящемся в пределах контролируемой зоны муниципального автономного общеобразовательного учреждения «Гимназия города Юрги».

ИСПДн 2 и ИСПДн 3 региональные (муниципальные) информационные сети, причем, благодаря использованию современной Интернет-технологии на всех уровнях, возможно получать информацию в режиме реального времени.

Связи между основными компонентами

В ИСПДн 1 персональные данные хранятся на рабочей станции (АРМ).

Данные вводятся на АРМ оператора.

В ИСПДн 2 и ИСПДн 3 персональные данные учащихся вводятся участниками образовательного процесса.

Режим и степень участия персонала в обработке персональных данных

В процессе обработки персональных данных участвуют следующие категории персонала:

Пользователь – осуществляет ввод персональных данных в ИСПДн. Он не имеет возможности вносить модификации в настройки какого-либо оборудования и программного обеспечения.

Администратор – занимается обслуживанием и настройкой АРМ и сетевого оборудования, поддержанием их работоспособности, резервном копировании данных. Он имеет полномочия устанавливать и разграничивать права доступа в защищенную инфраструктуру ИСПДн.

4. 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, обуславливающим 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 условие размещения технических средств ИСПДн.

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.

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 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):

- 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 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);

- 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, обуславливающих 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. Такое представление описывается следующей формализованной записью:

угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

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 (регистроваться) 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.

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) 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.)>.

6.1.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 нормативными документами Федеральной службы безопасности Российской Федерации в установленном ею порядке.

По наличию права постоянного или разового доступа в контролируемую зону (КЗ) 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, 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;
- осуществляет 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 съём 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.

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, 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 (винчестеры, микросхемы оперативной памяти, процессор, микросхемы и 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.).

6.2. 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 данных.

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 расходом 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.).

6.3. Общая характеристика угроз непосредственного доступа в операционную среду ИСПДн

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

- к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;
- в операционную среду, то есть в среду функционирования локальной операционной системы отдельного технического средства ИСПДн с возможностью выполнения несанкционированного доступа путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- в среду функционирования прикладных программ (например, к локальной системе управления базами данных);
- непосредственно к информации пользователя (к файлам, текстовой, аудио-и графической информации, полям и записям в электронных базах данных) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн.

6.4. Общая характеристика угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия

Если ИСПДн реализована на базе локальной или распределенной информационной системы, то в ней могут быть реализованы угрозы безопасности информации путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться НСД к ПДн или реализовываться угроза отказа в обслуживании. Особенно опасны угрозы, когда ИСПДн представляет собой распределенную информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена. В ее основу положено семь следующих первичных признаков классификации.

1. Характер угрозы. По этому признаку угрозы могут быть пассивные и активные. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу ИСПДн, но могут быть нарушены установленные правила разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации. Активная угроза – это угроза, связанная с воздействием на ресурсы ИСПДн, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т.д.), и с нарушением установленных правил разграничения доступа к ПДн или сетевым ресурсам. Примером таких угроз является угроза «Отказ в обслуживании», реализуемая как «шторм ТСР- запросов».

2. Цель реализации угрозы. По этому признаку угрозы могут быть направлены на нарушение конфиденциальности, целостности и доступности информации (в том числе на нарушение работоспособности ИСПДн или ее элементов).

3. Условие начала осуществления процесса реализации угрозы. По этому признаку может реализовываться угроза:

- по запросу от объекта, относительно которого реализуется угроза. В этом случае нарушитель ожидает передачи запроса определенного типа, который и будет условием начала осуществления несанкционированного доступа;
- по наступлению ожидаемого события на объекте, относительно которого реализуется угроза. В этом случае нарушитель осуществляет постоянное наблюдение за состоянием операционной системы ИСПДн и при возникновении определенного события в этой системе начинает несанкционированный доступ;
- безусловное воздействие. В этом случае начало осуществления несанкционированного доступа безусловно по отношению к цели доступа, то есть угроза реализуется немедленно и безотносительно к состоянию системы.

4. Наличие обратной связи с ИСПДн. По этому признаку процесс реализации угрозы может быть с обратной связью и без обратной связи. Угроза, осуществляемая при наличии обратной связи с ИСПДн, характеризуется тем, что на некоторые запросы, переданные на ИСПДн, нарушителю требуется получить ответ. Следовательно, между нарушителем и ИСПДн существует обратная связь, которая позволяет нарушителю адекватно реагировать на все изменения, происходящие в ИСПДн. В отличие от угроз, реализуемых при наличии обратной связи с ИСПДн, при реализации угроз без обратной связи не требуется реагировать на какие-либо изменения, происходящие в ИСПДн.

5. Расположение нарушителя относительно ИСПДн. В соответствии с этим признаком угроза реализуется как внутрисегментно, так и межсегментно.

Сегмент сети – физическое объединение хостов (технических средств ИСПДн или коммуникационных элементов, имеющих сетевой адрес). Например, сегмент ИСПДн образует совокупность хостов, подключенных к серверу по схеме «общая шина». В случае, когда имеет место внутрисегментная угроза, нарушитель имеет физический доступ к аппаратным элементам ИСПДн. Если имеет место межсегментная угроза, то нарушитель располагается вне ИСПДн, реализуя угрозу из другой сети или из другого сегмента ИСПДн.

6. Уровень эталонной модели взаимодействия открытых систем(ISO/OSI), на котором реализуется угроза. По этому признаку угроза может реализовываться на физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном уровне модели ISO/OSI.

7. Соотношение количества нарушителей и элементов ИСПДн, относительно которых реализуется угроза. По этому признаку угроза может быть отнесена к классу угроз, реализуемых одним нарушителем относительно одного технического средства ИСПДн (угроза «один к одному»), сразу относительно нескольких технических средств ИСПДн (угроза «один ко многим») или несколькими нарушителями с разных компьютеров относительно одного или нескольких технических средств ИСПДн (распределенные или комбинированные угрозы).

6.5. Общая характеристика угроз программно-математических воздействий

Программно-математическое воздействие – это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое не пустое подмножество следующих функций:

скрывать признаки своего присутствия в программной среде компьютера; обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

разрушать (искажать произвольным образом) код программ в оперативной памяти;

выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);

сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки.

Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИСПДн с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИСПДн.

Современные вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром деструктивных возможностей (от несанкционированного исследования параметров ИСПДн без вмешательства в функционирование ИСПДн, до уничтожения ПДн и программного обеспечения ИСПДн) и могут действовать во всех видах программного обеспечения (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

Наличие в ИСПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления

НСД.

К программным закладкам относятся программы, фрагменты кода, инструкции, формирующие не декларированные возможности программного обеспечения. Вредоносные программы могут переходить из одного вида в другой, например, программная закладка может сгенерировать программный вирус, который, в свою очередь, попав в условия сети, может сформировать сетевого червя или другую вредоносную программу, предназначенную для осуществления НСД.

Краткая характеристика основных вредоносных программ сводится к следующему. Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot- сектор. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора

диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т.е. на вирус) управление. После этого начинают выполняться инструкции вируса, который, как правило, уменьшает объем свободной памяти, копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть), перехватывает необходимые вектора прерываний (обычно – INT 13H), считывает в память оригинальный boot-сектор и передает на него управление.

В дальнейшем загрузочный вирус ведет себя так же, как файловый: перехватывает обращения операционной системы к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия, вызывает звуковые эффекты или видеоэффекты.

Основными деструктивными действиями, выполняемыми этими вирусами, являются:

- уничтожение информации в секторах дискет и винчестера;
- исключение возможности загрузки операционной системы (компьютер «зависает»);
- искажение кода загрузчика;
- форматирование дискет или логических дисков винчестера;
- закрытие доступа к СОМ-и LPT-портам;
- замена символов при печати текстов;
- подергивания экрана;
- изменение метки диска или дискеты;
- создание псевдосбойных кластеров;
- создание звуковых и (или) визуальных эффектов (например, падение букв на экране);
- порча файлов данных;
- перезагрузка компьютера;
- вывод на экран разнообразных сообщений;
- отключение периферийных устройств (например, клавиатуры);
- изменение палитры экрана;
- заполнение экрана посторонними символами или изображениями;
- погашение экрана и перевод в режим ожидания ввода с клавиатуры;
- шифрование секторов винчестера;
- выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
- уменьшение объема оперативной памяти;
- вызов печати содержимого экрана;
- блокирование записи на диск;
- уничтожение таблицы разбиения (Disk Partition Table), после этого компьютер можно загрузить только с флоппи-диска;
- блокирование запуска исполняемых файлов;
- блокирование доступа к винчестеру.

Большинство загрузочных вирусов перезаписывают себя на флоппи-диски. Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо операционной системы. По способу заражения файлов вирусы делятся на замещающие («overwriting»), паразитические («parasitic»), компаньон-вирусы («companion»),

«link»-вирусы, вирусы-черви и вирусы, заражающие объектные модули(OBJ), библиотеки компиляторов(LIB) и исходные тексты программ.

Метод заражения «overwriting» является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать. К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или

частично работоспособными.

Основными типами таких вирусов являются вирусы, записывающиеся в начало, середину или конец файлов. Отдельно следует отметить довольно незначительную группу паразитических вирусов, не имеющих «точки входа» (ЕРО-вирусы– Entry Point Obscuringviruses). К ним относятся вирусы, не записывающие команду передачи управления в заголовок .COM-файлов (JMP) и не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса.

Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и проявить себя только при некоторых ограниченных условиях.

К категории «компаньон» относятся вирусы, не изменяющие заражаемые файлы. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, то есть вирус. Наиболее распространены компаньон-вирусы, использующие особенность DOS первым выполнять файлы с расширением .COM, если в одном каталоге присутствуют два файла с одними тем же именем, но различными расширениями имени– .COM и .EXE. Такие вирусы создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла ХСОРУ.EXE создается файл ХСОРУ .COM. Вирус записывается в COM-файл и никак не изменяет EXE- файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, то есть вирус, который затем запустит и EXE-файл. Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл ХСОРУ .EXE переименовывается в ХСОРУ .EXD, а вирус записывается под именем ХСОРУ.EXE. При запуске управление получает код вируса, который затем запускает оригинальный ХСОРУ, хранящийся под именем ХСОРУ.EXD.

Интересен тот факт, что данный метод работает, по-видимому, во всех операционных системах. В третью группу входят так называемые «Path- companion» вирусы. Они либо записывают свой код под именем заражаемого файла, но «выше» на один уровень в прописываемых путях (DOS, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву на один подкаталог выше и т.д.

Возможно существование и других типов компаньон - вирусов, использующих иные оригинальные идеи или особенности других операционных систем.

Файловые черви (worms) являются, в некотором смысле, разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии–например, INSTALL.EXE или WINSTART.BAT.

Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и прочие). Некоторые вирусы записывают команду запуска зараженного файла в BAT- файлы. Не следует путать файловые вирусы-черви сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами .Link-вирусы, как и компаньон-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Вирусы, заражающие OBJ-и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и не способен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же «живого» вируса

становится СОМ-или ЕХЕ-файл. Получив управление файловый вирус совершает следующие общие действия:

- проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена (в случае, если вирус является резидентным), ищет незараженные файлы в текущем и (или) корневом каталоге путем сканирования дерева каталогов логических дисков, а затем заражает обнаруженные файлы;

- выполняет дополнительные (если они есть) функции: деструктивные действия, графические или звуковые эффекты и т.д. (дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий, в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счетчики и т.д.);

- возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо лечат файл, выполняют его, а затем снова заражают, либо восстанавливают программу (но не файл) в исходном виде (например, у СОМ-программы восстанавливается несколько первых байт, у ЕХЕ- программы вычисляется истинный стартовый адрес, у драйвера восстанавливаются значения адресов программ стратегии и прерывания).

Необходимо отметить, что чем быстрее распространяется вирус, тем вероятнее возникновение эпидемии этого вируса, чем медленнее распространяется вирус, тем сложнее его обнаружить (если, конечно же, этот вирус неизвестен).

Нерезидентные вирусы часто являются «медленными» – большинство из них при запуске заражает один или два-три файла и не успевает заполнить компьютер до запуска антивирусной программы (или появления новой версии антивируса, настроенной на данный вирус). Существуют, конечно же, нерезидентные «быстрые» вирусы, которые при запуске ищут и заражают все выполняемые файлы, однако такие вирусы очень заметны: при запуске каждого зараженного файла компьютер некоторое (иногда достаточно долгое) время активно работает с винчестером, что демаскирует вирус. Скорость распространения (инфицирования) у резидентных вирусов обычно выше, чем у нерезидентных - они заражают файлы при каких-либо обращениях к ним. В результате на диске оказываются зараженными все или почти все файлы, которые постоянно используются в работе. Скорость распространения (инфицирования) резидентных файловых вирусов, заражающих файлы только при их запуске на выполнение, будет ниже, чем у вирусов, заражающих файлы и при их открытии, переименовании, изменении атрибутов файла и т.д.

Таким образом, основные деструктивные действия, выполняемые файловыми вирусами, связаны с поражением файлов (чаще исполняемых или файлов данных), несанкционированным запуском различных команд (в том числе, команд форматирования, уничтожения, копирования и т.п.), изменением таблицы векторов прерываний и др. Вместе с тем, могут выполняться и многие деструктивные действия, сходные с теми, которые указывались для загрузочных вирусов.

Макровирусы (macro viruses) являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Наибольшее распространение получили макровирусы для пакета прикладных программ Microsoft Office.

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями:

- 1) привязки программы на макроязыке к конкретному файлу;
- 2) копирования макропрограмм из одного файла в другой;
- 3) получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют прикладные программы Microsoft Word, Excel и Microsoft Access. Они содержат в себе макроязыки: Word Basic, Visual Basic for Applications. При этом:

- 1) макропрограммы привязаны к конкретному файлу или находятся внутри файла;
- 2) макроязык позволяет копировать файлы или перемещать макропрограммы в служебные файлы системы и редактируемые файлы;
- 3) при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом или имеют стандартные имена.

Данная особенность макроязыков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый «автоматизированный документооборот». С другой стороны, возможности макроязыков таких систем позволяют вирусу переносить свой код в другие файлы и таким образом заражать их. Большинство макровирусов активны не только в момент открытия (закрытия) файла, но до тех пор, пока активен сам редактор. Они содержат все свои функции в виде стандартных макросов Word/Excel/Office. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не макросов. Известно три подобных приема, все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило, подобные вирусы имеют небольшой (иногда – полиморфный) макрос-загрузчик вируса, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает (чтобы скрыть следы присутствия вируса). Основной код таких вирусов присутствует либо в самом макросе вируса в виде текстовых строк (иногда – зашифрованных), либо хранится в области переменных документа.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

«Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла. Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недеklarированных возможностей программного и программно - аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

В связи с усложнением и возрастанием разнообразия программного обеспечения число вредоносных программ быстро возрастает. Сегодня известно более 120 тысяч сигнатур компьютерных вирусов. Вместе с тем, далеко не все из них представляют реальную угрозу. Во многих случаях устранение уязвимостей в системном или прикладном программном обеспечении привело к тому, что ряд вредоносных программ уже не способен внедриться в них. Часто основную опасность представляют новые вредоносные программы.

6.6. Общая характеристика результатов несанкционированного или случайного доступа

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);

- нарушению целостности (уничтожение, изменение);

- нарушению доступности (блокирование).

Нарушение конфиденциальности может быть осуществлено в случае утечки информации:

- копирования ее на отчуждаемые носители информации;

- передачи ее по каналам передачи данных;

- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;

- при «сборке мусора» нарушителем в процессе эксплуатации ИСПДн. Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

- микропрограммы, данные и драйвера устройств вычислительной системы;

- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;

- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;

- программы и данные прикладного программного обеспечения;

- программы и данные специального программного обеспечения;

- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы. Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

- конфигурацией сети;

- адресами и маршрутизацией передачи данных в сети;

- функциональным контролем сети;

- безопасностью информации в сети.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

- средств обработки информации;

- средств ввода/вывода информации;

- средств хранения информации;

- аппаратуры и каналов передачи;

- средств защиты информации.

7. Частная модель угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных

	ИСПДн1 ИСПДн2	ИСПДн3
По структуре	АРМ	Региональная Информационная сеть
Подключение к сетям связи общего пользования и (или) сетям международного информационного обмена	Имеет подключение	Имеет подключение
Режим обработки ПДн	Однопользовательская	Многопользовательская
По разграничению прав доступа пользователей	Без разграничения	С разграничением
В зависимости от местонахождения	Все технические средства находятся в пределах Российской Федерации	

7.1. Частная модель угроз безопасности персональных данных, обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

7.2. Частная модель угроз безопасности персональных данных обрабатываемых в региональных информационных системах персональных данных, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в региональных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для предыдущих типов ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включают в себя угрозы, аналогичные тем, которые реализуются в отдельном АРМ, не имеющем подключения к сетям связи общего пользования.

Угрозы из внешних сетей включают в себя:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб,
- открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

7.3. Вероятность реализации угроз для ИСПДн МАОУ «Гимназия города Юрги»

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	неактуальная
2.5. Угрозы несанкционированного доступа по каналам связи.	

2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за пределами контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3. Угрозы выявления паролей по сети	неактуальная
2.5.4. Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5. Угрозы подмены доверенного объекта в сети	актуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	актуальная
2.5.7. Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8. Угрозы удаленного запуска приложений	неактуальная
2.5.9. Угрозы внедрения по сети вредоносных программ	актуальная

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- установка антивирусной защиты;
- использование протокола защищенного соединения (HTTPS);
- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначение ответственного за обработку персональных данных из числа сотрудников Оператора;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- осуществление резервирования ключевых элементов ИСПДн;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.