Документ предоставлен [КонсультантПлюс](http://www.consultant.ru)

Утверждена

Заместителем директора

ФСТЭК России

14 февраля 2008 г.

МЕТОДИКА

ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ

ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ПЕРСОНАЛЬНЫХ ДАННЫХ

Введение

Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) разработана ФСТЭК России на основании Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781, с учетом действующих нормативных документов ФСТЭК России по защите информации. Методика предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных:

государственных или муниципальных ИСПДн;

ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями (далее - организациями) независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением;

ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

Документ предназначен для специалистов по обеспечению безопасности информации, руководителей организаций и предприятий, организующих и проводящих работы по обработке ПДн в ИСПДн.

1. Общие положения

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается 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.

В соответствии со статьей 19 Федерального закона N 152-ФЗ от 27 июля 2006 г. "О персональных данных" ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой ПДн по техническим каналам, приведено в "Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных". Выявление технических каналов утечки ПДн осуществляется на основе нормативных и методических документов ФСТЭК России.

Источниками угроз, реализуемых за счет несанкционированного доступа к базам данных с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПДн правила разграничения доступа к информации. Этими субъектами могут быть:

нарушитель;

носитель вредоносной программы;

аппаратная закладка.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам 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.

Для ИСПДн, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, терминальные устройства ИСПДн, подключенные к сетям общего пользования.

Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационным ресурсам ИСПДн и мер по контролю порядка проведения работ.

Угрозы несанкционированного доступа от внешних нарушителей реализуются с использованием протоколов межсетевого взаимодействия.

Детальное описание угроз, связанных с несанкционированным доступом в ИСПДн персональных данных, приведено в "Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных".

Выявление угроз НСД к ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса составляются специальные опросные листы.

Наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о наличии данной угрозы. Формируя на основе опроса перечень источников угроз ПДн, на основе опроса и сетевого сканирования перечень уязвимых звеньев ИСПДн, а также по данным обследования ИСПДн - перечень технических каналов утечки информации, определяются условия существования в ИСПДн угроз безопасности информации и составляется их полный перечень. На основании этого перечня в соответствии с описанным ниже порядком формируется перечень актуальных угроз безопасности ПДн.

2. Порядок определения актуальных угроз

безопасности персональных данных в информационных системах

персональных данных

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем.

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИСПДн и частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 1.

Таблица 1

Показатели исходной защищенности ИСПДн

┌────────────────────────────────┬────────────────────────────────────────┐

│ Технические и эксплуатационные │ Уровень защищенности │

│ характеристики ИСПДн ├─────────────┬────────────┬─────────────┤

│ │ высокий │ средний │ низкий │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│1. По территориальному │ │ │ │

│размещению: │ │ │ │

│распределенная ИСПДн, которая│ - │ - │ + │

│охватывает несколько областей,│ │ │ │

│краев, округов или государство│ │ │ │

│в целом; │ │ │ │

│городская ИСПДн, охватывающая│ - │ - │ + │

│не более одного населенного│ │ │ │

│пункта (города, поселка); │ │ │ │

│корпоративная распределенная│ - │ + │ - │

│ИСПДн, охватывающая многие│ │ │ │

│подразделения одной│ │ │ │

│организации; │ │ │ │

│локальная (кампусная) ИСПДн,│ - │ + │ - │

│развернутая в пределах│ │ │ │

│нескольких близко расположенных│ │ │ │

│зданий; │ │ │ │

│локальная ИСПДн, развернутая в│ + │ - │ - │

│пределах одного здания │ │ │ │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│2. По наличию соединения с│ │ │ │

│сетями общего пользования: │ │ │ │

│ИСПДн, имеющая многоточечный│ - │ - │ + │

│выход в сеть общего│ │ │ │

│пользования; │ │ │ │

│ИСПДн, имеющая одноточечный│ - │ + │ - │

│выход в сеть общего│ │ │ │

│пользования; │ │ │ │

│ИСПДн, физически отделенная от│ + │ - │ - │

│сети общего пользования │ │ │ │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│3. По встроенным (легальным)│ │ │ │

│операциям с записями баз│ │ │ │

│персональных данных: │ │ │ │

│чтение, поиск;│ + │ - │ - │

│запись, удаление, сортировка;│ - │ + │ - │

│модификация, передача│ - │ - │ + │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│4. По разграничению доступа к│ │ │ │

│персональным данным: │ │ │ │

│ИСПДн, к которой имеют доступ│ - │ + │ - │

│определенные перечнем│ │ │ │

│сотрудники организации,│ │ │ │

│являющейся владельцем ИСПДн,│ │ │ │

│либо субъект ПДн; │ │ │ │

│ИСПДн, к которой имеют доступ│ - │ - │ + │

│все сотрудники организации,│ │ │ │

│являющейся владельцем ИСПДн; │ │ │ │

│ИСПДн с открытым доступом │ - │ - │ + │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│5. По наличию соединений с│ │ │ │

│другими базами ПДн иных ИСПДн: │ │ │ │

│интегрированная ИСПДн│ - │ - │ + │

│(организация использует│ │ │ │

│несколько баз ПДн ИСПДн, при│ │ │ │

│этом организация не является│ │ │ │

│владельцем всех используемых│ │ │ │

│баз ПДн); │ │ │ │

│ИСПДн, в которой используется│ + │ - │ - │

│одна база ПДн, принадлежащая│ │ │ │

│организации - владельцу данной│ │ │ │

│ИСПДн │ │ │ │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│6. По уровню обобщения│ │ │ │

│(обезличивания) ПДн: │ │ │ │

│ИСПДн, в которой│ + │ - │ - │

│предоставляемые пользователю│ │ │ │

│данные являются обезличенными│ │ │ │

│(на уровне организации,│ │ │ │

│отрасли, области, региона и│ │ │ │

│т.д.); │ │ │ │

│ИСПДн, в которой данные│ - │ + │ - │

│обезличиваются только при│ │ │ │

│передаче в другие организации и│ │ │ │

│не обезличены при│ │ │ │

│предоставлении пользователю в│ │ │ │

│организации; │ │ │ │

│ИСПДн, в которой│ - │ - │ + │

│предоставляемые пользователю│ │ │ │

│данные не являются│ │ │ │

│обезличенными (т.е.│ │ │ │

│присутствует информация,│ │ │ │

│позволяющая идентифицировать│ │ │ │

│субъекта ПДн) │ │ │ │

├────────────────────────────────┼─────────────┼────────────┼─────────────┤

│7. По объему ПДн, которые│ │ │ │

│предоставляются сторонним│ │ │ │

│пользователям ИСПДн без│ │ │ │

│предварительной обработки: │ │ │ │

│ИСПДн, предоставляющая всю базу│ - │ - │ + │

│данных с ПДн; │ │ │ │

│ИСПДн, предоставляющая часть│ - │ + │ - │

│ПДн; │ │ │ │

│ИСПДн, не предоставляющая│ + │ - │ - │

│никакой информации │ │ │ │

└────────────────────────────────┴─────────────┴────────────┴─────────────┘

Исходная степень защищенности определяется следующим образом.

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу).

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по [пункту 1](#P154) и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по [пунктам 1](#P154) и [2](#P155).

 При составлении перечня актуальных угроз безопасности ПДн каждой

степени исходной защищенности ставится в соответствие числовой коэффициент

Y , а именно:

 1

0 - для высокой степени исходной защищенности;

5 - для средней степени исходной защищенности;

10 - для низкой степени исходной защищенности.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

 При составлении перечня актуальных угроз безопасности ПДн каждой

градации вероятности возникновения угрозы ставится в соответствие числовой

коэффициент Y , а именно:

 2

0 - для маловероятной угрозы;

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

 Y = (Y + Y ) / 20

 1 2

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если 0 </= Y </= 0,3, то возможность реализации угрозы признается низкой;

если 0,3 < Y </= 0,6, то возможность реализации угрозы признается средней;

если 0,6 < Y </= 0,8, то возможность реализации угрозы признается высокой;

если Y > 0,8, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 2.

Таблица 2

Правила отнесения угрозы безопасности ПДн к актуальной

|  |  |
| --- | --- |
|  Возможность  реализации  угрозы  |  Показатель опасности угрозы  |
|  низкая  |  средняя  |  высокая  |
| Низкая  | неактуальная  | неактуальная  | актуальная  |
| Средняя  | неактуальная  | актуальная  | актуальная  |
| Высокая  | актуальная  | актуальная  | актуальная  |
| Очень высокая  | актуальная  | актуальная  | актуальная  |

С использованием данных о классе ИСПДн и составленного перечня актуальных угроз, на основе "Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и "Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" формулируются конкретные организационно-технические требования по защите ИСПДн от утечки информации по техническим каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПДн.