Министерство связи и массовых коммуникаций Российской Федерации

ОДОБРЕНО

Решение секции №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2

МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В СПЕЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТРАСЛИ

СОГЛАСОВАНО

Письмо ФСБ России
от 10.08.2010 г. № 149/7/2/6-1203

СОГЛАСОВАНО

Письмо ФСТЭК России
от 04.06.2010 г. № 240/2/2271

Москва 2010

Перечень обозначений и сокращений

АРМ	–	автоматизированное рабочее место
ИР	–	информационный ресурс
ИСПДн	–	информационная система персональных данных
КЗ	–	контролируемая зона
ПДн	–	персональные данные
ПО	–	программное обеспечение
ПТС	–	программно-технические средства
ПЭМИН	–	побочные электромагнитные излучения и наводки
СЗИ	–	средства защиты информации
СКЗИ	–	средства криптографической защиты информации
ФСБ	–	Федеральная служба безопасности
ФСО	–	Федеральная служба охраны
ФСТЭК	–	Федеральная служба по техническому и экспертному контролю-

Содержание

Преамбула

Согласно постановлению Правительства Российской Федерации от 02 июня 2008 года № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации» Министерство связи и массовых коммуникаций Российской Федерации является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в следующих сферах:

– информационные технологии (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним);

– электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи;

– массовых коммуникаций и средств массовой информации (в том числе электронных), печати, издательской и полиграфической деятельности;

– обработки персональных данных.

Выделенный функционал с позиции отраслевого нормативного регулирования можно отнести к федеральным законам, формирующим правоотношения для сфер деятельности вышеназванного министерства:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ);

– Федеральный закон от 07 июля 2003 года № 126-ФЗ «О связи» (далее – Закон №126-ФЗ);

– Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» (далее – Закон № 2124-1);

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ).

Характеризуя вышеназванное законодательство по критерию распространяемости правоотношений на иные отрасли в связи с выделением общего предмета регулирования, необходимо отметить особенность сферы действия Закона № 149-ФЗ и Закона № 152-ФЗ. Регулируемые данными нормативными правовыми актами правоотношения касаются особенностей использования информации, в том числе персональной, применительно к различным сферам деятельности, и выделение типичных отраслевых признаков обработки персональных данных, выявленных при анализе данных законов, нецелесообразно.

В рамках данной модели при характеристике отдельной отрасли, использующей информационные системы персональных данных с возможностью последующей их типизации, предлагается остановиться на следующих критериях, при совокупном их использовании:

– основные признаки отрасли и виды оказываемых услуг внутри отрасли;

– полномочия субъектов, формирующих условия и особенности обработки персональных данных в отрасли, в том числе полномочия по вопросам формирования и ведения информационных систем, содержащих информацию, имеющую характер персональных данных;

– участники правоотношений в отрасли, определяемые отраслевой нормативной правовой базой;

– условия, установленные специальным законодательством, которые определяют особенности обработки информации, имеющей характер персональных данных, отдельных категорий субъектов персональных данных.

Наиболее наглядным примером выявления всех вышеперечисленных критериев обладает отрасль связи. Однако они также распространяются на сферу массовых коммуникаций и средств массовой информации, за исключением неавтоматизированной обработки персональных данных, выполняемой в соответствии с требованиями статьи 34 Закона № 2124-1.

Поэтому данная модель угроз применима при использовании и в указанной сфере при учете специфики процессов обработки персональных данных, выделяемых на основе вышеозначенных критериев.

1 Общие положения

Настоящая модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в специальных ИСПДн предприятий отрасли. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.

Модель является методическим документом и предназначена для операторов ПДн, разработчиков ИСПДн и их подсистем при разработке частных (детализированных) моделей угроз безопасности ПДн в отдельных ИСПДн конкретных предприятий с учетом их назначения, условий и особенностей функционирования.

В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн.

Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, приведенные в настоящей отраслевой Модели, подлежат адаптации в ходе разработки частных (детализированных) моделей угроз.

Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите персональных данных.

2 Характеристика объекта информатизации

В отрасли существуют следующие типы ИСПДн:

1. ИСПДн абонентов услуг связи (пользователей услугами связи).
2. ИСПДн о зарегистрированных владельцах радиоэлектронных средств.
3. ИСПДн пользователей радиочастотным спектром – единая база сбора, учета и хранения данных о присвоенных радиочастотах.
4. ИСПДн получателей разрешений на строительство и эксплуатацию линий связи при пересечении государственной границы Российской Федерации, на приграничной территории, во внутренних морских водах и в территориальном море Российской Федерации.
5. ИСПДн ведения бухгалтерского учета, управления персоналом, расчета заработной платы хозяйствующего субъекта отрасли и управления доступом.

В рамках **ИСПДн первого типа**:

– ведется обработка персональных данных абонентов (пользователей услугами связи);

– в некоторых случаях требуется заключение письменной формы договора;

– в некоторых случаях оператор связи сам устанавливает перечень обрабатываемой информации (включая персональные данные), в этом случае он не проверяет корректность предоставляемых абонентом данных;

– оператор связи проверяет корректность предоставляемых абонентом данных для возможности дальнейшего информационного взаимодействия с ним;

– ведется обработка персональных данных физических лиц – аффилированных лиц отрасли для предоставления сведений в реестр операторов, занимающих существенное положение в сети связи общего

пользования, который ведет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Операторами связи, вне зависимости от вида услуг, обрабатывается обязательный перечень информации, имеющей характер персональных данных абонентов (пользователей услугами связи):

- фамилия, имя, отчество;
- дата и место рождения;
- место жительства;
- реквизиты документа, удостоверяющего личность.

Кроме того, информация об абоненте, имеющая характер персональных данных, содержится в предоставляемых абонентом оператору связи документах:

- копия документа, подтверждающего право владения или пользования помещением, в котором устанавливается оборудование;
- письменное согласие законных представителей;
- доверенность.

Роскомнадзором обрабатывается обязательный перечень информации, имеющей характер персональных данных физических лиц – аффилированных лиц отрасли:

- фамилия, имя, отчество;
- должность;
- идентификационный номер налогоплательщика.

В рамках **ИСПДн второго типа**:

- ведется обработка персональных данных владельцев радиоэлектронных средств;
- требуется заключение письменной формы договора;
- оператор связи проверяет корректность предоставляемых абонентом данных для возможности информационного взаимодействия с ним.

Обрабатывается обязательный перечень информации, имеющей характер персональных данных заявителей – заказчиков системного проекта сети связи аккредитованным лицом:

– фамилия, имя, отчество заявителя;

– место жительства;

– реквизиты основного документа, удостоверяющего личность;

– идентификационный номер налогоплательщика.

Кроме того, к заявлению прилагаются следующие документы, содержащие информацию, имеющую характер персональных данных:

– системный проект сети связи и копия системного проекта, заверенная заявителем;

– копии задания на разработку системного проекта и исходные данные, заверенные подписью и печатью заказчика системного проекта или уполномоченного им лица, использовавшиеся для подготовки системного проекта;

– копии лицензий на оказание услуг связи, для которых предназначена проектируемая сеть связи;

– документы, подтверждающие полномочия заявителя действовать от имени заказчика системного проекта (если заявителем является уполномоченное заказчиком системного проекта лицо).

Роскомнадзором обрабатывается обязательный перечень информации, имеющей характер персональных данных владельцев радиоэлектронных средств и высокочастотных устройств:

– фамилия, имя, отчество;

– место жительства;

– данные документа, удостоверяющего личность гражданина Российской Федерации, включая номер и дату выдачи основного документа, удостоверяющего личность физического лица, и наименование органа, выдавшего этот документ.

К заявлению прилагаются документы, содержащие информацию, имеющую характер персональных данных:

– копия разрешения на использование радиочастот (радиочастотных каналов) для радиоэлектронных средств (в случае, если наличие такого разрешения предусмотрено законодательством Российской Федерации);

– копия документа, подтверждающего факт внесения записи об индивидуальном предпринимателе в Единый государственный реестр индивидуальных предпринимателей, – для индивидуальных предпринимателей;

– копия документа о присвоении позывного сигнала опознавания, если присвоение такого позывного сигнала предусмотрено Регламентом радиосвязи Международного союза электросвязи.

Роскомнадзор вносит в установленном порядке сведения о зарегистрированных радиоэлектронных средствах и высокочастотных устройствах в базу данных и выдает заявителю свидетельство о регистрации или мотивированное уведомление об отказе в такой регистрации.

В рамках **ИСПДн третьего типа**:

– ведется обработка персональных данных пользователей радиочастот или радиочастотных каналов;

– требуется заключение письменной формы договора;

– оператор связи проверяет корректность предоставляемых абонентом данных для возможности информационного взаимодействия с ним.

Радиочастотной службой, Государственной комиссией по радиочастотам, Роскомнадзором, обрабатывается обязательный перечень информации, имеющей характер персональных данных заявителей, о присвоении радиочастоты (радиочастотного канала) для радиоэлектронных средств гражданского назначения:

– фамилия, имя, отчество;

– место жительства (адрес места жительства);

– данные документа, удостоверяющего личность;

– контактная информация о заявителе (в том числе отдельно указаны телефон и факс);

– индивидуальный номер налогоплательщика.

Предприятиями осуществляется взаимодействие с Минобороны России, ФСО России, ФСБ России.

К заявлению, подаваемому в Роскомнадзор, прилагаются документы, содержащие информацию, имеющую характер персональных данных:

– копия соответствующего решения государственной комиссии по радиочастотам;

– пояснительная записка, в которой приводится обоснование запрашиваемого количества радиочастот или радиочастотных каналов; дается информация о назначении планируемой радиосети (радиолинии); о заявляемой деятельности; особенностях применяемых радиоэлектронных средств; условия совместного использования полос радиочастот с радиоэлектронными средствами военного назначения, а также другой информации, относящейся к данному вопросу;

– выписка из единого государственного реестра индивидуальных предпринимателей, заверенная органом, выдавшим указанный документ, или нотариально заверенная копия указанного документа.

В рамках **ИСПДн четвертого типа**:

– ведется обработка персональных данных получателей разрешений на строительство и эксплуатацию линий связи при пересечении государственной границы Российской Федерации, на приграничной территории, во внутренних морских водах и в территориальном море Российской Федерации;

– требуется заключение письменной формы договора;

– оператор связи проверяет корректность предоставляемых абонентом данных для возможности информационного взаимодействия с ним.

Роскомнадзором и иными уполномоченными органами государственной власти обрабатывается обязательный перечень информации, имеющей характер

персональных данных заявителей, о получении разрешения на строительство и эксплуатацию линий связи при пересечении государственной границы Российской Федерации на приграничной территории:

- фамилия, имя, отчество;
- место жительства;
- данные документа, удостоверяющего личность;
- индивидуальный номер налогоплательщика;
- почтовый адрес для переписки, контактные телефоны.

К заявлению прилагаются документы, содержащие информацию, имеющую характер персональных данных:

- копии лицензий на осуществление соответствующих видов деятельности и решений о предоставлении водных объектов в пользование в случаях, когда наличие таких лицензий и решений предусмотрено законодательством Российской Федерации;
- документы, подтверждающие наличие разрешений, предусмотренных законодательством Российской Федерации, – при проведении работ в полосе отвода автомобильных или железных дорог, нефте- и продуктопроводов, газопроводов, линий электропередачи и других технологических объектов, а также на территории пунктов пропуска через государственную границу Российской Федерации;
- сведения о всех формах и степени участия граждан Российской Федерации и (или) российских юридических лиц в проведении работ – для иностранных заявителей;
- сведения о лицах, привлекаемых заявителем к проведению работ, в том числе о работниках, участвующих в их проведении.

В рамках **ИСПДн пятого типа**:

- ведется обработка персональных данных работников хозяйствующего субъекта отрасли;

– ведется обработка персональных данных посетителей объектов размещения хозяйствующего субъекта отрасли;

Обрабатывается обязательный перечень информации, имеющей характер персональных данных работников хозяйствующего субъекта отрасли:

– фамилия, имя, отчество;
– фотография;
– гражданство;
– дата и место рождения;
– пол;
– реквизиты документа, удостоверяющего личность;
– место регистрации;
– состояние в браке;
– фамилия, имя, отчество супруга (-и), детей;
– количество детей;
– дата рождения детей;
– профессия;
– категория запаса;
– воинское звание и личный код;
– номер военного билета, удостоверения гражданина, подлежащего призыву на военную службу;
– полное обозначение военно-учетной специальности;
– категория годности к военной службе;
– военный комиссариат по месту жительства;
– номер команды, партии воинского учета;
– образование;
– наименование образовательного учреждения;
– номер и серия диплома;
– квалификация по документу об образовании;

– направление или специальность по документу;

– номер страхового свидетельства государственного пенсионного страхования.

Может обрабатываться дополнительный перечень информации, имеющей характер персональных данных работников, в соответствии с утвержденными нормативными правовыми актами Российской Федерации различного уровня в зависимости от организационно-правовой формы, особенностей налогового режима хозяйствующего субъекта отрасли.

Исходя из основных характеристик, особенностей отраслевых ИСПДн и решаемых ими задач в качестве объекта информатизации предприятия выступают:

1. Автономные автоматизированные рабочие места (АРМ).
2. Локальные вычислительные сети.
3. Распределенные вычислительные сети.

В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных предприятий подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

ИСПДн предполагают как распределенную (на АРМ), так и централизованную (на выделенных файловых серверах сети) обработку и хранение ПДн.

Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных клиентов предприятия другим предприятиям, внешним организациям, заинтересованным в создании собственных ИСПДн, как в электронном, так и в бумажном виде.

Контролируемой зоной (КЗ) ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места

пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3 Состав, категории и объем персональных данных

Состав персональных данных определяется соответствующим типом ИСПДн, описанных в разделе 2.

На основе характеристик и особенностей отрасли в части используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываемых в ИСПДн относятся как к персональным данным категории 3 (персональные данные, позволяющие идентифицировать субъекта персональных данных), так и к категории 2 (персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию). Кроме этого, в ИСПДн, используемых в сфере массовых коммуникаций, обрабатываются также персональные данные, относящихся к категории 4 (обезличенные и (или) общедоступные персональные данные).

Персональные данные категории 1 (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни) в ИСПДн отсутствуют.

Объемы ПДн, обрабатываемых в ИСПДн, для различных уровней реализации служебных процессов (федеральный, региональный, муниципальный, местный) в соответствии с «Порядком проведения классификации информационных систем персональных данных» могут быть трех типов:

1. **Группа Г1** – в ИСПДн находятся в процессе автоматизированной обработки персональные данные 100 000 и более либо данные субъектов в пределах субъекта Российской Федерации или Российской Федерации в целом;

2. **Группа Г2 –** в ИСПДн находятся в процессе автоматизированной обработки персональные данные от 1000 до 100 000 субъектов ПДн либо данные субъектов, в пределах отрасли Российской Федерации, в органе

государственной власти, проживающих в пределах муниципального образования;

3. **Группа Г3 –** в ИСПДн находятся в процессе автоматизированной обработки персональные данные менее 1000 субъектов ПДн или персональные данные субъектов ПДн, работающих в пределах конкретной организации.

4 Характеристики безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных

Учитывая особенности обработки ПДн, а также виды и категории обрабатываемой в ИСПДн персональных данных, основными характеристиками безопасности являются конфиденциальность, целостность и доступность, что в соответствии с «Порядком проведения классификации информационных систем персональных данных» характеризует указанные системы как специальные ИСПДн.

Под конфиденциальностью понимается обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания[1].

Под целостностью понимается состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения[2].

Под доступностью понимается состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов[3].

В дополнение к перечисленным выше основным характеристикам безопасности в ИСПДн могут рассматриваться также и другие характеристики безопасности:

---

[1] «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008 год.

[2] ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования»

[3] Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения»

– неотказуемость;

– учетность (подконтрольность);

– аутентичность;

– адекватность.

Под неотказуемостью понимается способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты[4].

Под учетностью (подконтрольностью) понимается обеспечение того, что действия субъекта по отношению к объекту (ПДн) могут быть прослежены уникально по отношению к субъекту[5].

Под аутентичностью понимается свойство, гарантирующее, что субъект или ресурс ПДн идентичны заявленным[6].

Под адекватностью понимается свойство соответствия преднамеренному поведению и результатам[7].

[4] ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

[5] «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», ФСБ России, 2008 год.

[6] ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

[7] «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», ФСБ России, 2008 год.

5 Классификация информационных систем персональных данных

Классификация ИСПДн осуществляется на основе анализа исходных данных о системе и обрабатываемых в ней персональных данных.

При проведении классификации ИСПДн необходимо учитывать следующие исходные данные:

- категория обрабатываемых в ИСПДн персональных данных;
- объем обрабатываемых в ИСПДн (персональные данные, находящие в ИСПДн в процессе автоматизированной обработки);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в ИСПДн.

ИСПДн относится к специальным системам, если в отношении обрабатываемых в ней персональных данных необходимо обеспечить выполнение не только одной характеристики безопасности, требуемой Федеральным законом «О персональных данных» – конфиденциальности, но и другие характеристики безопасности.

Кроме этого, существует еще один независимый критерий отнесения ИСПДн к специальным без учета наличия дополнительных характеристик безопасности персональных данных, а именно, наличие в информационной системе функций, предусматривающих принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Учитывая необходимость обязательного выполнения требований по обеспечению конфиденциальности персональных данных (за исключением общедоступных персональных данных), класс специальной информационной системы определяется в соответствии с таблицей 5.1.

Класс конкретной ИСПДн определяется на основании информации полученной в ходе комплексного анализа состояния деятельности отдельных предприятий в части организации работы с персональными данными,

осуществляемого на этапе разработки частных моделей угроз исходя из объемом, категорий и характеристики безопасности персональных данных, обрабатываемых в указанных ИСПДн. В случае обезличивания персональных данных ИСПДн может быть классифицирована как ИСПДн класса К4.

Таблица 5.1 – Классификация специальных информационных систем

Группа ПДн **Категория ПДн**	**Группа Г3**	**Группа Г2**	**Группа Г1**
Категория 3	специальная, К3	специальная, К3	специальная, К2
Категория 2	специальная, К3	специальная, К2	специальная, К1

Учитывая, что для различных ИСПДн могут иметь значимость различные характеристики безопасности ПДн, которые потребуют выработки дополнительных требований по защите персональных данных в ИСПДн, в классы специальных ИСПДн введены подклассы, характеризуемые появлением дополнительных характеристик безопасности.

Для этих целей каждой дополнительной характеристике ПДн в ИСПДн присваивается свой числовой индекс:

- целостность – 1;
- доступность – 2;
- неотказуемость – 3;
- учетность (подконтрольность) – 4;
- аутентичность – 5;
- адекватность – 6.

В результате, для ИСПДн, в которых необходимо обеспечение конфиденциальности и целостности, обрабатываемых в них персональных данных, присваивается подкласс аналогично примерам, приведенным в таблице 5.2. Аналогично осуществляется классификация по другим характеристикам безопасности.

В случае необходимости обеспечения нескольких дополнительных характеристик безопасности ПДн, требования к мерам и средствам защиты,

необходимым для реализации каждой их характеристик, суммируются и подкласс таких ИСПДн определяется аналогично примерам, приведенным в таблице 5.3.

Таблица 5.2 – Примеры подклассов специальных информационных систем с обязательным обеспечением характеристики безопасности (целостности)

Группа ПДн **Категория ПДн**	**Группа Г3**	**Группа Г2**	**Группа Г1**
Категория 3	специальная, К3-1	специальная, К3-1	специальная, К2-1
Категория 2	специальная, К3-1	специальная, К2-1	специальная, К1-1

Таблица 5.3 – Примеры подклассов специальных информационных систем с обязательным обеспечением трех характеристик безопасности (целостности, доступности и учетности)

Группа ПДн **Категория ПДн**	**Группа Г3**	**Группа Г2**	**Группа Г1**
Категория 3	специальная, К3-1.2.4	специальная, К3-1.2.4	специальная, К2-1.2.4
Категория 2	специальная, К3-1.2.4	специальная, К2-1.2.4	специальная, К1-1.2.4

6 Способы нарушения характеристик безопасности персональных данных

Исходя из перечня персональных данных, обрабатываемых в специальных ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:

- хищение персональных данных сотрудниками предприятия для использования в корыстных целях;
- передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
- несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам предприятия;
- несанкционированное получение персональных данных третьими лицами;
- уничтожение финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- модификация финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- блокирование финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- передача некорректной финансовой, адресной, юридической и прочей информации о субъекте ПДн;
- искажение архивной информации по субъекту ПДн.

7 Угрозы безопасности персональных данных, при их обработке в специальных информационных системах персональных данных

Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников предприятия в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:

- по видам возможных источников угроз;
- по типу ИСПДн, на которые направлена реализация угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по способам реализации угроз;
- по используемой уязвимости;
- по объекту воздействия.

Для специальных ИСПДн существуют следующие классы угроз безопасности ПДн:

По видам возможных источников угроз безопасности персональных данных

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

– угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;

– угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

Подробно источники угроз безопасности ПДн рассмотрены в подразделе 8 настоящей Модели.

По типу ИСПДн, на которые направлена угроза:

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

- угрозы безопасности данных, обрабатываемых в ИСПДн на базе автоматизированных рабочих мест;
- угрозы безопасности данных, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы безопасности данных, обрабатываемых в ИСПДн на базе распределенных систем.

По способам реализации угроз

По способам реализации угроз выделяют следующие классы угроз:

- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);
- угрозы специальных воздействий на ИСПДн.

По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными)

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс 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 воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
- угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

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.

При разработке частных (детализированных) моделей угроз должны учитываться подходы, изложенные в настоящей Модели, с детализацией угроз в соответствии с документом ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

8 Характеристика источников угроз безопасности персональных данных в ИСПДн

В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

Антропогенные источники угроз безопасности ПДн

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизация работы, вывод систем предприятия из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками предприятий отрасли, имеющих доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

– непредумышленное искажение или удаление программных компонентов;

– внедрение и использование неучтенных программ;

– игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:

- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;

- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников предприятия, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель) (в случае распределенных ИСПДн);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.

Техногенные источники угроз безопасности ПДн

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное программное обеспечение и аппаратные закладки.

Аппаратная закладка

Аппаратные закладки могут быть конструктивно встроенными и автономными.

Конструктивно встроенные аппаратные закладки создаются в ходе проектирования и разработки аппаратного обеспечения, применяемого в ИСПДн и могут проявляться в виде недекларированных возможностей различных элементов вычислительной системы.

Автономные аппаратные закладки являются законченными устройствами, выполняющими определенные функции перехвата, накопления, передачи или ввода/вывода информации. Например, функции автономной аппаратной закладки может выполнять сотовый телефон, несанкционированно подключаемый к ТС ИСПДн.

Учитывая, что аппаратные закладки представляют собой некоторый элемент технических средств (ТС), скрытно внедряемый или подключаемый к ИСПДн и обеспечивающий при определенных условиях реализацию несанкционированного доступа или непосредственное выполнение некоторых деструктивных действий, в них, как правило, содержатся микрокоманды, обеспечивающие взаимодействие закладки с программно-техническими средствами (ПТС) ИСПДн.

Аппаратные закладки могут реализовать угрозы:

- сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях (этапах) жизненного цикла ИСПДн.

Носитель вредоносной программы

В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства – видеоадаптера, сетевой платы, устройств ввода/вывода магнитных жестких, оптических и лазерных дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);
- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;
- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Стихийные источники угроз безопасности ПДн

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к предприятию. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при

наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Следует отметить, что, как правило, защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, в основном регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн и действующей нормативной базы Министерства.

9 Модель нарушителя безопасности персональных данных

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;

2. Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;

3. СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным)..

9.1 Описание нарушителей

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн все физические лица могут быть отнесены к следующим двум категориям:

- категория I – лица, не имеющие права доступа в контролируемую зону ИСПДн;
- категория II – лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;

– внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ.

В отношении ИСПДн в качестве внешнего нарушителями из числа лиц категории I могут выступать:

– бывшие сотрудники предприятий отрасли;
– посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
– представители преступных организаций.

Внешний нарушитель может осуществлять:

– перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
– деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
– несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
– перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами;
– атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

1. К **первой группе** относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;
- изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

2. Ко **второй группе** относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
- располагает ПДн, к которым имеет доступ.

3. К **третьей группе** относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной или распределенной сети предприятий.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;
- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

4. К **четвертой группе** относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн
- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
- имеет доступ ко всем техническим средствам сегмента ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

5. К **пятой группе** относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о ТС и конфигурации ИСПДн

– имеет доступ ко всем ТС ИСПДн и данным;
– обладает правами конфигурирования и административной настройки ТС ИСПДн.

6. К **шестой группе** относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

– 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).

7. К **седьмой группе** относятся лица из числа программистов-разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

– обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;
– может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

8. К **восьмой группе** относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

9.2 Предположения о возможностях нарушителя

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

В дополнении к приведенным в подразделе 9.2 возможностям, которыми обладают различные группы внутренних нарушителей, может быть приведен ряд дополнительных возможностей, которые присущи всем группам внутреннего нарушителя.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

9.3 Предположения об имеющихся у нарушителя средствах атак

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;

– штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

9.4 Описание каналов атак

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

– каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
– электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
– бумажные носители информации;
– штатные программно-аппаратные средства ИСПДн;
– кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно-техническими мерами;
– незащищенные каналы связи;
– ТКУИ.

9.5 Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации

При взаимодействии отдельных подсистем ИСПДн между собой по сетям связи общего пользования и (или) сетям международного информационного обмена, при обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами, а также при передаче ПДн по кабельным системам, расположенным в пределах контролируемой зоны и не защищенных от НСД к информации организационно-техническими мерами,

для обеспечения конфиденциальности и целостности информации необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей 9.1.

Таблица 9.1 – Соответствие типов нарушителя и класса СКЗИ

Группа внутреннего нарушителя	**Тип нарушителя**	**Класс СКЗИ**
Группа 1	H_2	КС2
Группа 2	H_3	КС3
Группа 3	H_3	КС3
Группа 4	H_3	КС3
Группа 5	H_3	КС3
Группа 6	H_3	КС3
Группа 7	H_5	КВ2
Группа 8	H_4	КВ1

Внешний нарушитель относится к типу H_1. При этом, если он обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа H_i (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа H_i ($2 \leq i \leq 6$).

Предполагается также, что возможности нарушителя типа H_{i+1} включают в себя возможности нарушителя типа H_i ($1 \leq i \leq 5$).

10 Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя:

- уровень исходной защищенности ИСПДн;
- частота (вероятность) реализации рассматриваемой угрозы.

10.1 Уровень исходной защищенности информационной системы персональных данных

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Перечень данных характеристик и показатели защищенности ИСПДн, зависящие от них, показаны в таблице 10.1[8]. Данный показатель рассчитывается для ИСПДн, исходя из обобщенных характеристик объекта информатизации.

Для определения исходной защищенности ИСПДн должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для ИСПДн.

Таблица 10.1 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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			

[8] В соответствии с положениями руководящего документа ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
локальная ИСПДн, развернутая в пределах одного здания			
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			
По встроенным (легальным) операциям с записями баз ПДн			
чтение, поиск			
запись, удаление, сортировка			
модификация, передача			
По разграничению доступа к персональным данным			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн			
ИСПДн с открытым доступом			
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			
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)			
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю базу данных с ПДн			
ИСПДн, предоставляющая часть ПДн			
ИСПДн, не предоставляющие никакой информации			
Количество решений			
Общее количество решений			

Принимается, что ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные уровню «средний».

В случае, если не менее 70% характеристик ИСПДн относится к уровню «не ниже среднего», а остальные к уровню «низкий», то исходная защищенность ИСПДн будет среднего уровня.

Во всех остальных случаях ИСПДн будет иметь низкий уровень защищенности.

10.2 Определение актуальных угроз безопасности персональных данных

Уровень исходной защищенности является первым параметром, используемым при оценке актуальности угроз безопасности ПДн, обрабатываемых в ИСПДн.

Для оценки уровня исходной защищенности, в соответствии с руководящим документом ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», вводится коэффициент исходной защищенности Y_1, который может принимать значения:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Следующим параметром, необходимым для определения актуальности угроз безопасности ПДн, является частота (или вероятность) реализации угрозы, под которой понимается определенный экспертным путем показатель, характеризующий вероятность реализации конкретной угрозы безопасности ПДн для ИСПДн в реальных условиях ее функционирования. Вводится четыре значения этого показателя, обозначаемого как Y_2:

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.

Данный показатель принимает следующие значения:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Используя значения приведенных выше показателей Y_1 и Y_2, вычисляется *коэффициент реализуемости угрозы* Y, определяемый соотношением $Y = (Y_1+Y_2)/20$.

В зависимости от своего значения этот коэффициент принимает значения:

$0 < Y < 0,3$ – реализуемость угрозы признается *низкой*;

$0,3 < Y < 0,6$ – реализуемость угрозы признается *средней*;

$0,6 < Y < 0,8$ – реализуемость угрозы признается *высокой*;

$Y > 0,8$ – реализуемость угрозы признается очень *высокой*.

Далее дается *оценка опасности* каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации. Данная оценка имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

После просчета всех показателей производится оценка актуальности каждой угрозы безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице 10.2:

Таблица 10.2 – Матрица расчета актуальности угроз безопасности ПДн

Реализуемость угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основании положений модели угроз, модели нарушителя, данных об исходной защищенности ИСПДн (Y_1), коэффициенте реализуемости угрозы (Y), вероятности ее реализации (Y_2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы безопасности ПДн, обрабатываемых в ИСПДн.

11 Заключение

Данная Модель, являясь методическим документом, представляет собой основу для разработки частных (детализированных) моделей угроз безопасности ПДн для специальных ИСПДн конкретных предприятий или их групп с учетом назначения, условий и особенностей функционирования, учитывающих:

- структуру информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы,

а также провести оценку актуальности угроз безопасности персональных данных.

Основные положения Модели должны быть детализированы при разработке частных (детализированных) моделей с учетом документов ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».