Действующая редакция

Постановление Администрации Смоленской области от 19.01.2018 № 15

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений

АДМИНИСТРАЦИЯ СМОЛЕНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 19 января 2018 года № 15

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных», Концепцией защиты информации на территории Смоленской области на период 2014-2020 годов, утвержденной постановлением Администрации Смоленской области от 11 декабря 2014 года № 848, в целях обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений,

Администрация Смоленской области постановляет:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений, согласно приложению к настоящему постановлению.

2. Органам исполнительной власти Смоленской области и подведомственным им учреждениям:

2.1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в используемых ими информационных системах персональных данных.

2.2. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться настоящим постановлением.

3. Рекомендовать органам местного самоуправления муниципальных образований Смоленской области руководствоваться настоящим постановлением при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных.

Губернатор
Смоленской области
А.В. Островский

Приложение
к постановлению Администрации
Смоленской области
от 19.01.2018 № 15

УГРОЗЫ БЕЗОПАСНОСТИ
персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных органов исполнительной власти Смоленской области и подведомственных им учреждений (далее также - актуальные угрозы), определены в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

1.2. Под угрозами безопасности персональных данных при их обработке в информационных системах персональных данных (далее также - ИСПДн) понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных).

1.3. В качестве источников угроз безопасности персональных данных могут выступать субъекты (физические лица, организации) или явления (техногенные

аварии, стихийные бедствия, иные природные явления). При этом источники угроз безопасности персональных данных могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);

- техногенные источники (техногенные угрозы);

- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

Источниками антропогенных угроз безопасности персональных данных могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к персональным данным (воздействия на персональные данные), содержащимся (содержащиеся) в ИСПДн, или нарушения функционирования ИСПДн или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

- лица, имеющие доступ к ИСПДн, непреднамеренные действия которых могут привести к нарушению безопасности персональных данных (непреднамеренные угрозы безопасности персональных данных).

Преднамеренные угрозы безопасности персональных данных могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

1.4. Актуальные угрозы содержат перечень актуальных угроз безопасности персональных данных, которые могут быть реализованы в типовых ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки, а также содержат совокупность предположении о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для рассматриваемых типов ИСПДн, в случае применения в ИСПДн средств криптографической защиты информации (далее также - СКЗИ).

Актуальные угрозы устанавливают единый подход к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и разработке на их основе частных моделей угроз безопасности персональных данных (далее - частные модели угроз) для этих ИСПДн.

1.5. При определении актуальных угроз использованы:

- Федеральный закон «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон «О персональных данных»;

- постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановление Администрации Смоленской области от 28.07.2003 № 190 «О Комиссии по информационной безопасности при Администрации Смоленской области»;

- постановление Администрации Смоленской области от 11.12.2014 № 848 «Об утверждении Концепции защиты информации на территории Смоленской области на период 2014 - 2020 годов»;

- постановление Администрации Смоленской области от 20.07.2015 № 424 «О порядке использования распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области»;

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15.02.2008;

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 14.02.2008;

- методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации 31.03.2015 № 149/7/2/6-432.

1.6. Актуальные угрозы безопасности персональных данных определяются по результатам оценки возможностей нарушителей, уровня исходной защищенности ИСПДн, анализа возможных способов реализации угроз безопасности персональных данных и последствий нарушения свойств безопасности персональных данных.

1.7. Источниками данных об угрозах безопасности информации, на основе которых определяются актуальные угрозы, являются:

- банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (http://bdu.fstec.ru);

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15.02.2008;

- методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра Федеральной службы безопасности Российской Федерации 31.03.2015 № 149/7/2/6-432.

В качестве источника данных об угрозах безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн органов исполнительной власти Смоленской области и подведомственных им учреждений, используются актуальные угрозы.

1.8. Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, осуществляется органами исполнительной власти Смоленской области и подведомственными им учреждениями, в случае если они являются операторами ИСПДн (далее - операторы).

Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, является обязательным и оформляется документально в виде частной модели угроз, которая утверждается руководителем оператора.

Частная модель угроз должна содержать:

- описание ИСПДн и особенностей ее функционирования, в том числе цель и задачи, решаемые посредством ИСПДн, структурно-функциональные характеристики ИСПДн (тип, к которому отнесена ИСПДн), физические и логические границы ИСПДн, применяемые в ней информационные технологии, сегменты ИСПДн и их типизацию, взаимосвязи между сегментами ИСПДн и другими информационными системами и информационно-телекоммуникационными сетями, в том числе информационно-телекоммуникационной сетью «Интернет» (далее - сеть «Интернет»), описание технологий обработки информации в ИСПДн, информацию о возможных уязвимостях ИСПДн;

- границы контролируемой зоны (контролируемых зон отдельных сегментов) ИСПДн;

- категории и объем обрабатываемых персональных данных, а также тип актуальных угроз безопасности персональных данных и уровень защищенности персональных данных;

- обеспечиваемые характеристики безопасности обрабатываемых персональных данных (конфиденциальность, целостность, доступность) и последствия нарушения указанных характеристик;

- исходный уровень защищенности ИСПДн;

- возможности нарушителей, в том числе типы и виды нарушителей, возможные цели и потенциал нарушителей;

- возможные способы реализации угроз безопасности персональных данных;

- обоснование необходимости (или отсутствия таковой) применения для обеспечения безопасности персональных данных СКЗИ, а также угрозы безопасности информации, актуальные в случае применения СКЗИ;

- актуальные угрозы безопасности персональных данных.

Разработка частной модели угроз осуществляется оператором самостоятельно и (или) с привлечением юридических лиц или индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, в соответствии с требованиями федерального законодательства и с обязательным использованием актуальных угроз. Актуальные угрозы подлежат адаптации операторами в ходе определения угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, с учетом структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДн.

1.9. В случае если оператором принято решение о применении СКЗИ для обеспечения безопасности персональных данных в ИСПДн, то при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в данной ИСПДн, оператор дополнительно формирует совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак.

1.10. Согласование операторами угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, а также частных моделей угроз, разработанных с использованием актуальных угроз, с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, не требуется.

1.11. Актуальные угрозы подлежат пересмотру по решению Комиссии по информационной безопасности при Администрации Смоленской области, а также в случае:

- изменения федерального законодательства в части определения угроз безопасности персональных данных, актуальных при их обработке в ИСПДн;

- появления новых угроз в используемых источниках данных об угрозах безопасности информации, которые будут актуальными для рассматриваемых типов ИСПДн;

- изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДн, следствием которого стало возникновение новых актуальных угроз безопасности персональных данных;

- повышения возможности реализации или опасности существующих угроз безопасности персональных данных;

- появления сведений и фактов о новых возможностях нарушителей.

2. Описание информационных систем персональных данных и особенностей их функционирования

2.1. Операторы эксплуатируют ИСПДн при осуществлении деятельности, связанной с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций.

2.2. В ИСПДн обрабатываются персональные данные различных категорий и объема, которые принадлежат субъектам персональных данных, являющимся как сотрудниками оператора, так и иными лицами.

В зависимости от состава и объема обрабатываемых персональных данных, а также типа актуальных угроз безопасности персональных данных, приведенного в пункте 4.2 раздела 4 актуальных угроз, в соответствии с пунктами 8-12 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, в ИСПДн необходимо обеспечение не выше чем второго уровня защищенности персональных данных.

Категория и объем обрабатываемых в ИСПДн персональных данных, а также уровень защищенности персональных данных для этих ИСПДн определяются их операторами, оформляются актом классификации ИСПДн и утверждаются руководителем оператора.

2.3. В зависимости от характера и способов обработки персональных данных операторы осуществляют их обработку в ИСПДн, которые имеют различную структуру (разноплановые ИСПДн).

По структуре ИСПДн подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети «Интернет», ИСПДн подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

По режиму обработки информации ИСПДн подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей ИСПДн подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

2.4. В ИСПДн могут применяться технологии виртуализации, клиент (файл)-серверные технологии, виртуальные частные сети (VPN), удаленный доступ, веб-технологии, кластеризация, сегментирование. При этом в ИСПДн не применяются технологии автоматизации управления технологическим процессом, облачные технологии, технологии больших данных, беспроводные сети связи, мобильные устройства, суперкомпьютеры и грид-вычисления, посредством которых могут возникнуть дополнительные угрозы безопасности персональных данных.

Факт применения (использования) каждой из таких информационных технологий или структурно-функциональных характеристик в ИСПДн должен быть отражен оператором в частной модели угроз.

2.5. Особенностью эксплуатации ИСПДн в органах исполнительной власти Смоленской области и подведомственных им учреждениях является использование единой информационно-телекоммуникационной инфраструктуры - распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее - РМС СО), сегментированной на территориальном, канальном и логическом уровнях, имеющей централизованное управление, систему мониторинга и оповещения о критических событиях, одноточечное подключение к сетям связи общего пользования и сети «Интернет». Содержание и порядок использования РМС СО, условия и порядок подключения органов исполнительной власти Смоленской области, органов местного самоуправления муниципальных образований Смоленской области, иных органов государственной власти и организаций к РМС СО, размещения информационных систем в РМС СО и обеспечения их безопасности определены Положением о РМС СО, утвержденным постановлением Администрации Смоленской области от 20.07.2015 № 424.

2.6. Технические средства ИСПДн находятся в пределах Российской Федерации. Контролируемой зоной ИСПДн являются административные здания или отдельные помещения операторов. В пределах контролируемой зоны находятся рабочие места пользователей, серверное оборудование, а также сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны могут находиться линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи. Неконтролируемое

пребывание посторонних лиц и неконтролируемый вынос за пределы зданий технических средств ИСПДн исключены.

2.7. Помещения, в которых ведется обработка персональных данных (далее – помещения), оснащены входными дверями с замками. Операторами установлен порядок доступа в помещения, препятствующий возможности неконтролируемого проникновения в помещения или пребывания в помещениях лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в помещения, а также в нерабочее время двери помещений закрываются на ключ. Доступ посторонних лиц в помещения допускается только в присутствии лиц, имеющих право самостоятельного доступа в помещения, на время, ограниченное служебной необходимостью. При этом операторами предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через устройства ввода/вывода информации, а также возможность доступа к носителям персональных данных.

Устройства ввода/вывода информации, участвующие в обработке персональных данных, располагаются в помещениях таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в помещение, а также через двери и окна помещения.

2.8. Ввод персональных данных в ИСПДн и вывод персональных данных из ИСПДн осуществляются с использованием бумажных и машинных носителей информации, в том числе отчуждаемых машинных носителей информации. Операторами устанавливается порядок, обеспечивающий сохранность используемых машинных носителей персональных данных, осуществляется их поэкземплярный учет.

2.9. В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных операторы определяют порядок и осуществляют резервирование персональных данных с использованием машинных носителей. В наличии имеются комплекты восстановления на применяемое в ИСПДн системное и прикладное программное обеспечение, а также средства защиты информации. Для ключевых элементов ИСПДн предусмотрены источники резервного электропитания, при необходимости применяются системы вентиляции и кондиционирования воздуха. Помещения оснащены средствами пожарной сигнализации.

2.10. Приняты меры по защите информации на технических средствах ИСПДн, направленные на:

- исключение возможности загрузки технических средств с внешних носителей, несанкционированного доступа к настройкам BIOS, использования встроенных адаптеров беспроводной связи (Wi-Fi, Bluetooth и др.);

- автоматическую установку критических обновлений операционной системы (согласно рекомендациям разработчика операционной системы);

- минимизацию привилегии пользователей;

- исключение возможности изменения состава и конфигурации программных и технических средств компьютера без санкции администратора;

- применение сертифицированных средств антивирусной защиты информации в соответствии с установленным оператором порядком.

2.11. В ИСПДн, имеющих подключение к РМС СО, реализовано одноточечное подключение к сетям общего пользования и сети «Интернет» через централизованный и защищенный канал оператора РМС СО с использованием средств разграничения доступа в виде межсетевых экранов. Доступ пользователей к ресурсам сети «Интернет» осуществляется посредством прокси-сервера, сертифицированного на соответствие требованиям безопасности информации, установленным федеральным законодательством. Реализована система обнаружения и предупреждения вторжений.

2.12. В ИСПДн в целях обеспечения безопасности персональных данных при их передаче по сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе сети «Интернет», применяются сертифицированные Федеральной службой безопасности Российской Федерации СКЗИ. Обоснование необходимости (или отсутствия таковой) применения СКЗИ для обеспечения безопасности персональных данных в ИСПДн осуществляется ее оператором в разрабатываемой для этой ИСПДн частной модели угроз.

Операторами, применяющими СКЗИ, устанавливается порядок, обеспечивающий сохранность документации на СКЗИ, машинных носителей информации с комплектами восстановления СКЗИ, а также носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и носители хранятся только в помещениях в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц.

2.13. Операторами используется единый подход к организации парольной защиты. Требования к составу, уникальности и управлению сроком действия пароля, порядок реагирования на инциденты, связанные с компрометацией паролей, определены оператором РМС СО.

2.14. С учетом особенностей функционирования, используемых структурно-функциональных характеристик и применяемых информационных технологий, а также опасности реализации угроз безопасности персональных данных и наступления последствий в результате несанкционированного или случайного доступа можно выделить следующие типы разноплановых ИСПДн, эксплуатируемых в органах исполнительной власти Смоленской области и подведомственных им учреждениях:

- 1-й тип - автоматизированные рабочие места, не имеющие подключения к сетям связи, в том числе к беспроводным сетям связи;

- 2-й тип - автоматизированные рабочие места, имеющие подключение к сетям связи, включая РМС СО, сети связи общего пользования и (или) сеть «Интернет»;

- 3-й тип - локальные ИСПДн (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, объединенного в единую информационную систему в пределах одного здания), имеющие подключение к сетям связи, включая РМС СО, сети связи общего пользования и (или) сеть «Интернет»;

- 4-й тип - распределенные ИСПДн, имеющие подключение к РМС СО, сети связи общего пользования и (или) сети «Интернет».

Актуальные угрозы безопасности персональных данных рассматриваются применительно к перечисленным типам разноплановых ИСПДн. При разработке частной модели угроз оператор мотивированно соотносит ИСПДн с одним из рассматриваемых типов.

2.15. К объектам защиты в ИСПДн относятся:

- персональные данные;

- носители персональных данных;

- средства защиты информации (в том числе СКЗИ);

- среда функционирования средств защиты информации (в том числе СКЗИ);

- ключевая, парольная и аутентифицирующая информация пользователей ИСПДн;

- носители ключевой, парольной и аутентифицирующей информации пользователей ИСПДн;

- документы, в которых отражена информация о мерах и средствах защиты ИСПДн;

- помещения, в которых осуществляется обработка персональных данных и (или) размещены компоненты ИСПДн;

- каналы (линии) связи.

2.16. В ИСПДн обработка информации осуществляется в однопользовательском и многопользовательском режимах. Осуществляется разграничение прав доступа пользователей ИСПДн. Обслуживание технических и программных средств ИСПДн, средств защиты информации, в том числе СКЗИ и среды их функционирования, включая настройку, конфигурирование и распределение носителей ключевой информации между пользователями ИСПДн, осуществляется привилегированными пользователями (системные администраторы, ответственные за обеспечение безопасности персональных данных, администраторы безопасности информации), назначенными оператором ИСПДн из числа доверенных лиц.

2.17. ИСПДн с учетом их структурно-функциональных характеристик и условий эксплуатации, а также применяемых информационных технологий и предпринятых мер обеспечения безопасности персональных данных, указанных в настоящем разделе, имеют средний уровень исходной защищенности.

2.18. Операторы на постоянной основе реализуют меры обеспечения безопасности персональных данных, приведенные в настоящем разделе.

3. Оценка возможностей реализации нарушителями угроз безопасности персональных данных

3.1. Нарушителем является физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИСПДн. С учетом наличия прав доступа и возможностей доступа к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители - лица, не имеющие права доступа к ИСПДн, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ ИСПДн;

- внутренние нарушители - лица, имеющие право постоянного или разового доступа к ИСПДн, ее отдельным компонентам.

3.2. С учетом состава и объема обрабатываемых персональных данных в ИСПДн, а также целей и задач их обработки в качестве возможных целей (мотивации) реализации нарушителями угроз безопасности персональных данных в ИСПДн могут быть:

- получение выгоды путем мошенничества или иным преступным путем;

- выявление уязвимостей с целью дальнейшей продажи уязвимостей и получения финансовой выгоды;

- любопытство или желание самореализации (подтверждение статуса);

- месть за ранее совершенные действия;

- непреднамеренные, неосторожные или неквалифицированные действия.

3.3. Предположения о возможных целях (мотивации) реализации угроз безопасности персональных данных для ИСПДн с заданными структурно-функциональными характеристиками и особенностями функционирования с учетом состава и объема обрабатываемых персональных данных в ИСПДн, целей и задач их обработки приведены в таблице.

Таблица

Тип ИСПДн	Вид нарушителя	Тип нарушителя	Возможные цели (мотивация) реализации угроз
1	**2**	**3**	**4**
1 -4	лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных видов работ	внутренний	получение выгоды путем мошенничества или иным преступным путем; непреднамеренные, неосторожные или неквалифицированные действия
1 -4	лица, обслуживающие инфраструктуру оператора (охрана, уборщики и т.д.)	внутренний	получение выгоды путем мошенничества или иным преступным путем; непреднамеренные, неосторожные или неквалифицированные действия
1 -4	пользователи ИСПДн	внутренний	получение выгоды путем мошенничества или иным преступным путем; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия
2-4	преступные группы (криминальные структуры)	внешний	- получение выгоды путем мошенничества или иным преступным путем;

			выявление уязвимостей с целью дальнейшей продажи уязвимостей и получения финансовой выгоды
2-4	внешние субъекты (физические лица)	внешний	- получение выгоды путем мошенничества или иным преступным путем; любопытство или желание самореализации (подтверждение статуса); выявление уязвимостей с целью дальнейшей продажи уязвимостей и получения финансовой выгоды
2-4	бывшие работники (пользователи)	внешний	получение выгоды путем мошенничества или иным преступным путем; месть за ранее совершенные действия

3.4. С учетом имеющейся совокупности предположений о целях (мотивации) нарушителей и возможностях реализации нарушителями угроз безопасности персональных данных в ИСПДн потенциал нападения при реализации угроз безопасности персональных данных для рассматриваемых видов нарушителей определяется как базовый (низкий).

Нарушитель с базовым (низким) потенциалом является непрофессионалом, использует стандартное оборудование, имеет ограниченные знания об ИСПДн или совсем их не имеет, возможность доступа к ИСПДн или ее отдельным компонентам у нарушителя ограничена и контролируется организационными и техническими мерами.

3.5. В ИСПДн угрозы безопасности персональных данных могут быть реализованы внешними и внутренними нарушителями с базовым (низким) потенциалом следующими способами:

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах);

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на общесистемном уровне (операционные системы, гипервизоры);

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на прикладном уровне (системы управления базами данных, браузеры, веб-приложения, иные прикладные программы общего и специального назначения);

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), кроме ИСПДн 1-го типа;

- несанкционированный физический доступ к объектам защиты и (или) воздействие на объекты защиты.

4. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

4.1. Угрозы безопасности персональных данных являются актуальными для ИСПДн, если существует вероятность их реализации нарушителем с базовым (низким) потенциалом и такая реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности обрабатываемых персональных данных.

4.2. Учитывая средний уровень исходной защищенности ИСПДн, состав и объем обрабатываемых в ИСПДн персональных данных, а также особенности их обработки, для ИСПДн органов исполнительной власти Смоленской области и подведомственных им учреждений в соответствии с пунктом 7 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, актуальны угрозы безопасности персональных данных 3-го типа.

4.3. С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринятых операторами мер по обеспечению безопасности персональных данных, приведенных в разделе 2 актуальных угроз, а также возможных негативных последствий от их реализации преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн являются неактуальными, вследствие чего далее из преднамеренных угроз безопасности персональных данных будут рассматриваться только угрозы, реализуемые за счет несанкционированного доступа.

4.4. К базовым угрозам безопасности персональных данных для рассматриваемых типов ИСПДн относятся угрозы, информация о которых получена из источников данных об угрозах безопасности информации, указанных в пункте 1.7 раздела 1 актуальных угроз, реализуемые внутренними и внешними нарушителями с базовым (низким) потенциалом.

В качестве базовых угроз безопасности персональных данных для ИСПДн операторами рассматриваются актуальные угрозы безопасности персональных данных при их обработке в рассматриваемых типах ИСПДн, перечень которых приведен в приложении № 1 к актуальным угрозам. При этом исключение могут составлять угрозы безопасности персональных данных, информационные технологии или структурно-функциональные характеристики для формирования которых в ИСПДн не применяются.

Базовый (предварительный) перечень рассматриваемых угроз безопасности персональных данных для ИСПДн приводится операторами в разрабатываемой для соответствующей ИСПДн частной модели угроз.

4.5. Оценка возможности реализации и актуальности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн, осуществляется операторами в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора Федеральной службы по техническому и экспортному контролю 14.02.2008, и приводится в частной модели угроз.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных.

Для оценки возможности реализации угрозы применяются следующие показатели:

- уровень исходной защищенности ИСПДн;

- частота (вероятность) реализации рассматриваемой угрозы.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности персональных данных для данной ИСПДн в складывающихся условиях. С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн частота (вероятность) реализации угроз безопасности персональных данных для типовых ИСПДн органов исполнительной власти Смоленской области и подведомственных им учреждений оценивается не выше средней.

Опасность угроз безопасности персональных данных определяется экспертным путем и характеризуется возможными негативными последствиями от их реализации для оператора и субъектов персональных данных. С учетом состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также необходимости обеспечения уровня защищенности персональных данных не выше второго опасность угроз безопасности персональных данных для типовых ИСПДн органов исполнительной власти Смоленской области и подведомственных им учреждений оценивается не выше средней.

Оценка возможности реализации и актуальности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн,

осуществляется операторами с учетом максимальных приведенных оценочных значений частоты (вероятности) реализации и опасности угроз.

4.6. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн органов исполнительной власти Смоленской области и подведомственных им учреждений, в которых для обеспечения безопасности персональных данных операторами принято решение о применении СКЗИ, приведена в приложении № 2 к актуальным угрозам и учитывает базовый (низкий) потенциал возможных нарушителей и предпринятые операторами меры по обеспечению безопасности персональных данных.

Совокупность предположений о возможностях, которые могут использовать нарушители при создании способов, подготовке и проведении атак на ИСПДн, в которых для обеспечения безопасности персональных данных операторами принято решение о применении СКЗИ, формируется операторами на основании приложения № 2 к актуальным угрозам и приводится в разрабатываемой для соответствующей ИСПДн частной модели угроз.

Примечание изготовителя базы данных: приложения №№ 1-2 сохранены во вложенном файле.