АДМИНИСТРАЦИЯ СМОЛЕНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

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

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 п о с т а н о в л я е т:

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 предположений 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

1	2	3	4
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.

Приложение № 1
к угрозам безопасности
персональных данных, актуальным
при обработке персональных
данных в информационных
системах персональных данных
органов исполнительной власти
Смоленской области и
подведомственных им учреждений

ПЕРЕЧЕНЬ
актуальных угроз безопасности персональных данных при их обработке в рассматриваемых типах ИСПДн

№ п/п	Угрозы безопасности информации				Последствия		
	идентификатор	наименование	описание	источник угрозы (характеристика и потенциал нарушителя)	нарушение конфиденциальности	нарушение целостности	нарушение доступности
1	2	3	4	5	6	7	8
1.	УБИ.006	угроза внедрения кода или данных	угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен пользователями вручную или автоматически при выполнении определенного условия (при наступлении определенной даты, входе пользователя в систему и т.п.), а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, то есть незаконного использования чужих вычислительных ресурсов.	внешний нарушитель с низким потенциалом	есть	есть	есть

1	2	3	4	5	6	7	8
			Данная угроза обусловлена наличием уязвимостей программного обеспечения, а также слабостями мер антивирусной защиты. Реализация данной угрозы возможна в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников, или при наличии у него привилегий установки программного обеспечения				
2.	УБИ.008	угроза восстановления аутентификационной информации	угроза заключается в возможности подбора (например, путем полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учетной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объемом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: - время подбора в основном определяется не объемом аутентификационной информации, а объемом данных ее хеш-кода; - восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – вручную	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
3.	УБИ.015	угроза доступа к защищаемым файлам с использованием обходного пути	угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при: - наличии у нарушителя прав доступа к некоторым объектам файловой системы; - отсутствии проверки вводимых пользователем данных; - наличии у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с ее помощью	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
4.	УБИ.028	угроза использования альтернативных путей доступа к ресурсам	угроза заключается в возможности получения нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: - возможности ввода произвольных данных в адресную строку; - сведений о пути к защищаемому ресурсу; - возможности изменения интерфейса ввода входных данных	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет

1	2	3	4	5	6	7	8
5.	УБИ.030	угроза использования информации идентификации/ аутентификации, заданной по умолчанию	угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учетной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учетные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: - при наличии у нарушителя сведений о производителе/модели объекта защиты и наличии в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учетной записи «по умолчанию» для объекта защиты; - при успешном завершении нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты	внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть
6.	УБИ.031	угроза использования механизмов авторизации для повышения привилегий	угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учетных записей с более высокими, чем у нарушителя, привилегиями, за счет ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
7.	УБИ.041	угроза межсайтового скриптинга	угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что вредоносный код будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	внешний нарушитель с низким потенциалом	есть	есть	есть

1	2	3	4	5	6	7	8
8.	УБИ.051	угроза невозможности восстановления сессии работы на компьютере при выводе из промежуточных состояний питания	угроза заключается в возможности потери несохраненных данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания (ждущего режима работы, гибернации и других)	внутренний нарушитель с низким потенциалом	нет	есть	есть
9.	УБИ.062	угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключенный к браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация данной угрозы возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга	внешний нарушитель с низким потенциалом	есть	нет	нет
10.	УБИ.067	угроза неправомерного ознакомления с защищаемой информацией	угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего ее использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путем просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путем подслушивания разговоров и другими способами	внутренний нарушитель с низким потенциалом	есть	нет	нет
11.	УБИ.069	угроза неправомерных действий в каналах связи	угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путем добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	внешний нарушитель с низким потенциалом	есть	есть	нет

1	2	3	4	5	6	7	8
12.	УБИ.071	угроза несанкционированного восстановления удаленной защищаемой информации	угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удаленная с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: - если удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); - если технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; - если информация не хранилась в криптографически преобразованном виде	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
13.	УБИ.074	угроза несанкционированного доступа к аутентификационной информации	угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
14.	УБИ.084	угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски, являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путем логического объединения нескольких виртуальных устройств хранения данных. Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства.	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть

1	2	3	4	5	6	7	8
			Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)				
15.	УБИ.086	угроза несанкционированного изменения аутентификационной информации	угроза заключается в возможности осуществления нарушителем неправомерного доступа к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учетной записью дискредитированного пользователя	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	нет	есть	есть
16.	УБИ.088	угроза несанкционированного копирования защищаемой информации	угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путем проведения последовательности неправомерных действий, включающих несанкционированный доступ к защищаемой информации, копирование найденной информации на съемный носитель или в другое место, доступное нарушителю вне системы. Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемую зону. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	нет	нет
17.	УБИ.089	угроза несанкционированного редактирования реестра	угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, но и любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть

1	2	3	4	5	6	7	8
18.	УБИ.090	угроза несанкционированного создания учетной записи пользователя	угроза заключается в возможности создания нарушителем в системе дополнительной учетной записи пользователя и ее дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учетной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удаленном доступе), или штатных средств управления доступом из состава операционной системы (при локальном доступе)	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть
19.	УБИ.091	угроза несанкционированного удаления защищаемой информации	угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путем осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующем данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	нет	нет	есть
20.	УБИ.098	угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (так называемое сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить, по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	внешний нарушитель с низким потенциалом	есть	нет	нет

1	2	3	4	5	6	7	8
21.	УБИ.099	угроза обнаружения хостов	угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющими клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	внешний нарушитель с низким потенциалом	есть	нет	нет
22.	УБИ.116	угроза перехвата данных, передаваемых по вычислительной сети	угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (то есть прослушивания сетевого трафика) для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз. При этом нарушитель остается при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в случае: - наличия у нарушителя доступа к дискредитируемой вычислительной сети; - неспособности технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	внешний нарушитель с низким потенциалом	есть	нет	нет
23.	УБИ.128	угроза подмены доверенного пользователя	угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять прием/передачу данных от его имени. Данную угрозу можно охарактеризовать как имитацию действий клиента. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств и типе используемого программного обеспечения	внешний нарушитель с низким потенциалом	есть	нет	нет

1	2	3	4	5	6	7	8
24.	УБИ.156	угроза утраты носителей информации	угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или ее потери (в случае отсутствия резервной копии данных). Данная угроза обусловлена слабостями мер регистрации и учета носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	внутренний нарушитель с низким потенциалом	есть	нет	есть
25.	УБИ.157	угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съемным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	внешний нарушитель с низким потенциалом	нет	есть	есть
26.	УБИ.159	угроза «форсированного веб-браузинга»	угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнению привилегированных операций или осуществлению иных деструктивных воздействий на некорректно защищенные компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации ручного ввода в адресную строку веб-браузера определенных адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	внешний нарушитель с низким потенциалом	есть	нет	нет
27.	УБИ.167	угроза заражения компьютера при посещении неблагонадежных сайтов	угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадежным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадежным содержимым	внутренний нарушитель с низким потенциалом	есть	есть	есть

1	2	3	4	5	6	7	8
28.	УБИ.168	угроза «кражи» учетной записи доступа к сетевым сервисам	угроза заключается в возможности неправомерного ознакомления нарушителя с защищаемой информацией пользователя путем получения информации идентификации/аутентификации, соответствующей учетной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условии: - наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учетная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего его отключили); - наличия у нарушителя сведений об адресе электронной почты, с которым связана учетная запись дискредитируемого пользователя для доступа к сетевым сервисам	внешний нарушитель с низким потенциалом	есть	нет	есть
29.	УБИ.170	угроза неправомерного шифрования информации	угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов	внешний нарушитель с низким потенциалом	нет	нет	есть
30.	УБИ.171	угроза скрытного включения вычислительного устройства в состав бот-сети	угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств и др.), подключенных к сети «Интернет», за счет захвата управления такими устройствами путем несанкционированной установки на них: - вредоносного программного обеспечения типа Backdoor для обеспечения нарушителя возможностью удаленного доступа к дискредитируемым вычислительным устройствам и удаленного управления ими; - клиентского программного обеспечения для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа «отказ в обслуживании» и др.). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть «Интернет»	внешний нарушитель с низким потенциалом	нет	нет	есть

1	2	3	4	5	6	7	8
31.	УБИ.172	угроза распространения «почтовых червей»	угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя	внешний нарушитель с низким потенциалом	есть	есть	есть
32.	УБИ.174	угроза «фарминга»	угроза заключается в возможности неправомерного ознакомления нарушителя с защищаемой информацией (в том числе идентификации/аутентификации) пользователя путем скрытного перенаправления пользователя на поддельный сайт (внешне идентичный оригинальному), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - специальных программных средств типа «эксплойт», реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа	внешний нарушитель с низким потенциалом	есть	нет	нет
33.	УБИ.175	угроза «фишинга»	угроза заключается в возможности неправомерного ознакомления нарушителя с защищаемой информацией (в том числе идентификации/аутентификации) пользователя путем убеждения пользователя с помощью методов социальной инженерии (в том числе посредством рассылки целевых писем (spear-phishing attack), с помощью звонков, стимулирующих к открытию вложения письма, имитации рекламных предложений (fake offers) или различных приложений (fake apps) зайти на поддельный сайт (внешне идентичный оригинальному), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть в письме зараженное вложение.	внешний нарушитель с низким потенциалом	есть	нет	нет

1	2	3	4	5	6	7	8
			Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга». Реализация данной угрозы возможна при условии наличия у нарушителя: - сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; - средств создания и запуска поддельного сайта; - сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)				
34.	УБИ.178	угроза несанкционированного использования системных и сетевых утилит	угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счет использования имеющихся или предварительно внедренных стандартных (известных и обычно не определяемых антивирусными программами как вредоносные) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условии: - наличия в системе стандартных системных и сетевых утилит или успешного их внедрения нарушителем в систему и сокрытия (с использованием существующих архивов, атрибутов «скрытый» или «только для чтения» и др.); - наличия у нарушителя привилегий на запуск таких утилит	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть
35.	УБИ.191	угроза внедрения вредоносного кода в дистрибутив программного обеспечения	угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть
36.	УБИ.192	угроза использования уязвимых версий программного обеспечения	угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	есть	есть	есть

Приложение № 2
к угрозам безопасности
персональных данных, актуальным
при обработке персональных
данных в информационных
системах персональных данных
органов исполнительной власти
Смоленской области и
подведомственных им учреждений

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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) угроз для построения и реализации атак	Обоснование отсутствия актуальности
1	2	3	4
1.	Проведение атаки при нахождении в пределах контролируемой зоны	актуально	-
2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты среды функционирования СКЗИ; - помещения, в которых находятся компоненты ИСПДн, на которых реализованы СКЗИ и среда функционирования СКЗИ	неактуально	проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверями с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения в эти помещения или пребывания в них лиц, не имеющих права доступа в эти помещения. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения, на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты.

1	2	3	4
			Установлен порядок, обеспечивающий сохранность документации на СКЗИ, машинных носителей информации с комплектами восстановления СКЗИ, носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и указанные носители хранятся только в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы ИСПДн; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИСПДн; - сведений о мерах по разграничению доступа в помещения, в которых находятся компоненты ИСПДн, на которых реализованы СКЗИ и среда функционирования СКЗИ	актуально	-
4.	Использование штатных средств ИСПДн, в которой используется СКЗИ, ограниченное реализованными в ИСПДн мерами, направленными на предотвращение и пресечение несанкционированных действий	актуально	-
5.	Физический доступ к компонентам ИСПДн, на которых реализованы СКЗИ и среда функционирования	неактуально	проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверями с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания в них лиц, не имеющих права доступа в эти помещения. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения, на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты

1	2	3	4
6.	Возможность воздействовать на аппаратные компоненты СКЗИ и среду функционирования СКЗИ, ограниченная мерами, реализованными в ИСПДн, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий	неактуально	базового (низкого) потенциала нарушителя недостаточно для реализации угрозы. Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными дверями с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания в них лиц, не имеющих права доступа в эти помещения. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения, на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты. Осуществляется разграничение, регистрация и учет доступа пользователей ИСПДн к объектам защиты с использованием организационных мер и средств ИСПДн. Правами управления (администрирования) ИСПДн обладают только привилегированные пользователи
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среды функционирования СКЗИ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения	неактуально	не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Для ИСПДн актуальны угрозы безопасности персональных данных 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении
8.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИСПДн, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий	неактуально	не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности

1	2	3	4
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования СКЗИ, в том числе с использованием исходных текстов входящего в среду функционирования прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ	неактуально	не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
10.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения	неактуально	для ИСПДн угрозы, связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении, неактуальны. Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Для ИСПДн актуальны угрозы безопасности персональных данных 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении
11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования СКЗИ	неактуально	не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Отсутствует в наличии конструкторская документация на аппаратные и программные компоненты среды функционирования СКЗИ
12.	Возможность воздействовать на любые компоненты СКЗИ и среды функционирования СКЗИ	неактуально	не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы