ПРАВИТЕЛЬСТВО БРЯНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 3 декабря 2018 г. № 623-п
г. Брянск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций, Правительство Брянской области
ПОСТАНОВЛЯЕТ:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций, согласно приложению.

2. Исполнительным органам государственной власти Брянской области и подведомственным им организациям для информационных систем персональных данных, операторами которых являются соответственно исполнительные органы государственной власти Брянской области и подведомственные им организации, осуществлять определение актуальных угроз безопасности персональных данных, а также разработку частных моделей угроз безопасности персональных данных, руководствуясь настоящим постановлением.

3. Исполнительным органам государственной власти Брянской области обеспечить доведение постановления до подведомственных организаций и его реализацию в данных подведомственных организациях.

4. Рекомендовать органам местного самоуправления Брянской области и подведомственным им организациям осуществлять определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, операторами которых они являются, и разработку частных моделей угроз безопасности персональных данных, руководствуясь данным постановлением.

5. Контроль за исполнением постановления возложить на заместителя Губернатора Брянской области Сергеева С.А.

Исполняющий обязанности
Губернатора А.Г. Резунов

Приложение
к постановлению Правительства
Брянской области
от 3 декабря 2018 г. № 623-п

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций

1. Общие положения

1.1. В настоящем документе используются термины и понятия, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методиками и методическими документами, утвержденными Федеральной службой по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) и Федеральной службой безопасности Российской Федерации (далее – ФСБ России).

1.2. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций (далее – актуальные угрозы), определены в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.3. Под актуальными угрозами безопасности персональных данных 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.

Для информационных систем персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций (далее – ИСПДн) целью защиты информации является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

1.4. 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 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 в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

лица, имеющие доступ к информационной системе, 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 информационной системы, технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

1.5. Настоящие 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. Актуальные угрозы также содержат совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для рассматриваемых типов ИСПДн, в случае применения в них для обеспечения безопасности персональных данных средств криптографической защиты информации (далее – СКЗИ).

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

1.6. Актуальные угрозы безопасности персональных данных определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, уровня исходной защищенности ИСПДн, анализа возможных способов реализации угроз безопасности персональных данных и последствий от нарушения свойств безопасности персональных данных (конфиденциальности, целостности, доступности).

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

банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) (далее – банк данных угроз);

базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 года (далее – базовая модель угроз).

1.8. Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, осуществляется исполнительными органами государственной власти Брянской области и подведомственными им организациями соответственно, в случае если они являются операторами ИСПДн (далее – операторы).

Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, является обязательным для их операторов и оформляется документально в виде частных моделей угроз, которые утверждаются руководителем оператора.

1.9. В случае если оператором принято решение применения 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. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и разработке частных моделей угроз для этих ИСПДн использование настоящих актуальных угроз операторами обязательно.

Настоящие актуальные угрозы применяются на этапах создания ИСПДн для определения и оценки угроз безопасности персональных данных, а также в ходе эксплуатации ИСПДн при периодическом пересмотре (переоценке) угроз безопасности персональных данных.

1.11. Настоящие актуальные угрозы подлежат адаптации операторами в ходе определения угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн.

Адаптация актуальных угроз направлена на уточнение (уменьшение) перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и осуществляется с учетом их структурно-функциональных характеристик, применяемых информационных технологий и особенностей функционирования (в том числе исключение угроз, которые непосредственно связаны с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн).

1.12. В рамках одной частной модели угроз операторам рекомендуется рассматривать угрозы безопасности персональных данных только для одной ИСПДн.

1.13. Частная модель угроз должна содержать:

описание ИСПДн и особенностей ее функционирования, в том числе цель и задачи, решаемые 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 с сетью «Интернет», технологии обработки информации в ИСПДн, возможные уязвимости ИСПДн;

границы контролируемой зоны (контролируемых зон отдельных сегментов) ИСПДн;

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

обеспечиваемые характеристики безопасности обрабатываемых персональных данных (конфиденциальность, целостность, доступность) и последствия от их нарушения;

исходный уровень защищенности ИСПДн;

оценку возможностей (типа, вида, потенциала) нарушителей, необходимых им для реализации угроз безопасности персональных данных;

возможные способы реализации угроз безопасности персональных данных;

обоснование необходимости (или отсутствия таковой) применения для обеспечения безопасности персональных данных СКЗИ;

совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, в случае применения в ИСПДн для обеспечения безопасности персональных данных СКЗИ и определение требуемого класса СКЗИ;

актуальные угрозы безопасности персональных данных.

1.14. В случае если ИСПДн имеет сегменты, которые эксплуатируют иные органы государственной власти, органы местного самоуправления или организации, то определение угроз безопасности персональных данных, актуальных при обработке персональных данных в такой ИСПДн, с учетом всех имеющихся сегментов осуществляется ее оператором.

1.15. Для определения угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и разработки частных моделей угроз операторами могут привлекаться юридические лица или индивидуальные предприниматели, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

1.16. Согласование операторами угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн,

и частных моделей угроз, разработанных с использованием настоящих 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.

1.17. Настоящие актуальные угрозы подлежат пересмотру (переоценке):

при изменении законодательства Российской Федерации в части определения угроз безопасности персональных данных при их обработке в информационных системах;

при появлении новых угроз в источниках данных об угрозах безопасности информации, используемых в настоящих актуальных угрозах, которые будут актуальными для рассматриваемых типов ИСПДн;

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

при повышении возможности реализации или опасности существующих угроз безопасности персональных данных;

при появлении сведений и фактов о новых возможностях нарушителей.

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, подлежат пересмотру (переоценке) оператором:

при внесении изменений в настоящие актуальные угрозы для соответствующего типа ИСПДн;

при изменении структурно-функциональных характеристик или особенностей функционирования ИСПДн, вследствие чего изменился тип, к которому относится ИСПДн;

при применении в ИСПДн информационных технологий, посредством которых могут формироваться новые угрозы безопасности персональных данных, исключенные из базового (предварительного) перечня угроз безопасности персональных данных для этой ИСПДн оператором;

при повышении возможности реализации существующих угроз безопасности персональных данных;

в иных случаях по решению оператора.

2. Структура информационных систем персональных данных

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

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

В зависимости от состава (категории) и объема обрабатываемых персональных данных, а также типа актуальных угроз безопасности персональных данных, приведенного в пункте 4.2 настоящих актуальных угроз, в ИСПДн необходимо обеспечение не выше чем второго уровня защищенности персональных данных.

Категория и объем персональных данных, обрабатываемых в ИСПДн, а также уровень защищенности персональных данных, который необходимо обеспечить для этих ИСПДн, определяются их операторами, оформляются документально 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), беспроводные сети связи, удаленный доступ, веб-технологии, кластеризация, сегментирование, мобильные устройства. При этом в ИСПДн не применяются технологии автоматизации управления технологическим процессом, облачные технологии, технологии больших данных, суперкомпьютеры и грид-вычисления, посредством которых могут формироваться дополнительные угрозы безопасности персональных данных.

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

2.5. 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:

автоматизированные рабочие места (далее – АРМ), не имеющие подключения (незащищенного, защищенного) к каким-либо сетям связи,

в том числе к беспроводным сетям связи (исключение составляют беспроводные технологии, предназначенные для функционирования периферийных устройств (клавиатура, манипулятор «мышь» и другие), входящих в состав АРМ) (тип 1);

АРМ, имеющие подключение к сетям связи, включая сети связи общего пользования и (или) сети международного информационного обмена, в том числе сеть «Интернет» (тип 2);

локальные ИСПДн (комплекс АРМ, объединенных в единую информационную систему посредством выделенной сети связи в пределах одного здания), не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена (тип 3);

локальные ИСПДн (комплекс АРМ, объединенных в единую информационную систему в пределах одного здания), имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети «Интернет» (тип 4);

распределенные ИСПДн (комплекс АРМ и (или) локальных информационных систем, объединенных в единую информационную систему посредством выделенной сети связи и территориально разнесенных между собой), не имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена (тип 5);

распределенные ИСПДн (комплекс АРМ и (или) локальных информационных систем, объединенных в единую информационную систему и территориально разнесенных между собой), имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети «Интернет» (тип 6).

Далее актуальные угрозы будут рассматриваться применительно к перечисленным типам разноплановых ИСПДн.

2.6. При определении угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, оператор мотивированно соотносит данную ИСПДн с одним из 6 рассматриваемых типов в разрабатываемой для этой ИСПДн частной модели угроз. При этом ИСПДн не допускается относить к типам 3 и 5, в частности, если:

ИСПДн имеет подключение (незащищенное, защищенное) к сетям связи и (или) информационным системам (в том числе иных операторов), которые имеют свое подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети «Интернет»;

в ИСПДн осуществляется передача какой-либо информации посредством сети связи (незащищенной, защищенной), предоставляемой иным органом государственной власти или организацией, в том числе оператором связи, если им не гарантируется предоставление выделенной сети связи;

ИСПДн имеет подключение к беспроводным сетям связи (исключение составляют беспроводные технологии, предназначенные для функционирования периферийных устройств (клавиатура, манипулятор «мышь» и другие),

входящих в состав АРМ), и оператором не предприняты меры по обеспечению безопасности обрабатываемых персональных данных от несанкционированного или случайного доступа посредством данных сетей связи;

оператором не предпринимаются меры по недопущению несанкционированного подключения ИСПДн к сетям связи, в том числе к беспроводным сетям связи.

В случае отнесения ИСПДн к типам 3 и 5 оператору в частной модели угроз необходимо дополнительно привести мотивированное обоснование отнесения применяемой сети связи в такой ИСПДн к категории выделенной.

2.7. 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 и неконтролируемый вынос за пределы административных зданий технических средств ИСПДн исключены.

2.8. Помещения, в которых ведется обработка персональных данных (далее – помещения), оснащены входными дверьми с замками. Операторами установлен порядок доступа в помещения, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в помещение, а также в нерабочее время двери помещения закрываются на ключ. Доступ посторонних лиц в помещения допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные 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 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.

2.9. Ввод (вывод) персональных данных в ИСПДн осуществляется с использованием бумажных и машинных носителей информации, в том числе съемных машинных носителей информации (магнитные и оптические диски, флеш-накопители, накопители на жестких магнитных дисках, твердотельные накопители и другие) (далее – машинные носители персональных данных).

Операторами установлен порядок, обеспечивающий сохранность используемых машинных носителей персональных данных, осуществляется

их поэкземплярный учет. Хранятся машинные носители персональных данных только в помещениях в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц. Выдача машинных носителей персональных данных осуществляется под подпись только сотрудникам, допущенным к обработке персональных данных.

2.10. В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных операторы осуществляют их резервирование в соответствии с установленным порядком с использованием машинных носителей персональных данных. 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.

2.11. 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 адаптеров беспроводной связи (Wi-Fi, Bluetooth и др.);

установку критических обновлений операционной системы;

минимизацию привилегий пользователей;

исключение возможности несанкционированного изменения состава и конфигурации программных и технических средств автоматизированного рабочего места;

обеспечение антивирусного контроля в ИСПДн в соответствии с установленным оператором порядком с применением сертифицированных средств антивирусной защиты информации.

2.12. Операторами используется единый подход к организации парольной защиты. Требования к составу, уникальности, сроку действия пароля, порядок реагирования на инциденты, связанные с компрометацией паролей, определены оператором.

2.13. 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 ФСБ России СКЗИ.

Указанные СКЗИ допускается не применять в следующих случаях:

если передача персональных данных осуществляется по выделенной сети связи в ИСПДн типов 3 и 5 и оператором предприняты меры по защите передаваемых персональных данных от перехвата нарушителем;

если в ИСПДн (сегменте ИСПДн) или между ИСПДн передача персональных данных осуществляется по сети связи (за исключением сетей связи международного информационного обмена, в том числе сети «Интер-

нет»), в пределах границ контролируемой зоны и оператором предприняты меры по защите передаваемых по сети связи персональных данных от перехвата нарушителем;

если в ИСПДн (сегменте ИСПДн) или между ИСПДн передача персональных данных, в том числе за пределы границ контролируемой зоны, осуществляется посредством виртуальной частной сети (VPN), предоставляемой оператором связи при оказании услуги связи оператору в соответствии с Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи» на основании заключенного государственного контракта или договора.

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.

2.14. Операторами, применяющими СКЗИ, устанавливается порядок, обеспечивающий сохранность документаций 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.

2.15. В ИСПДн обработка информации осуществляется в однопользовательском и многопользовательском режимах. Осуществляется разграничение прав доступа (набора действий, разрешенных для выполнения) пользователей. 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), которые назначаются из числа доверенных лиц. Операторами назначены (определены) сотрудники (структурные подразделения), ответственные за обеспечение безопасности персональных данных в ИСПДн.

2.16. К объектам защиты в ИСПДн относятся:

обрабатываемые персональные данные;

машинные носители персональных данных;

средства защиты информации, в том числе СКЗИ;

среда функционирования средств защиты информации, в том числе СКЗИ;

информация, относящаяся к защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию;

носители ключевой, парольной и аутентифицирующей информации;

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

помещения;

каналы (линии) связи.

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 для имеющихся ИСПДн на постоянной основе должны обеспечивать меры обеспечения безопасности персональных данных, приведенные в настоящем разделе.

3. Оценка возможностей нарушителей по реализации 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.

В зависимости от права разового или постоянного доступа в контролируемую зону и возможностей по доступу к обрабатываемым персональным данным и (или) к компонентам ИСПДн рассматриваются нарушители двух типов:

внешние нарушители – лица, не имеющие права доступа к ИСПДн или ее отдельным компонентам;

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

3.2. С учетом состава (категории) 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;

любопытство или желание самореализации;

реализация угроз безопасности персональных данных из мести;

реализация угроз безопасности персональных данных непреднамеренно из-за неосторожности или неквалифицированных действий.

3.3. Для ИСПДн типов 1, 3 и 5 с заданными структурно-функциональными характеристиками и особенностями функционирования (осуществляется разграничение прав доступа пользователей), а также с учетом сделанных предположений (прогноза) о возможных целях (мотивации) реализации угроз безопасности персональных данных рассматриваются следующие виды нарушителей:

лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, – внутренние нарушители;

лица, обслуживающие инфраструктуру оператора (охрана, уборщики и т.д.), – внутренние нарушители;

пользователи ИСПДн – внутренние нарушители.

Для ИСПДн типов 2, 4 и 6 рассматриваются следующие виды нарушителей:

преступные группы (криминальные структуры) – внешние нарушители;

внешние субъекты (физические лица) – внешние нарушители;

лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, – внутренние нарушители;

лица, обслуживающие инфраструктуру оператора (охрана, уборщики и т.д.), – внутренние нарушители;

пользователи ИСПДн – внутренние нарушители;

бывшие сотрудники (пользователи) – внешние нарушители.

3.4. Нарушители обладают следующими возможностями по реализации угроз безопасности персональных данных в ИСПДн:

получать информацию об уязвимостях отдельных компонентов ИСПДн, опубликованную в общедоступных источниках;

получать информацию о методах и средствах реализации угроз безопасности персональных данных (компьютерных атак), опубликованных в общедоступных источниках;

самостоятельно осуществлять создание способов атак, подготовку и проведение атак на ИСПДн только за пределами контролируемой зоны;

самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом и без физического доступа к ИСПДн или ее отдельным компонентам, на которых реализованы меры и средства защиты информации, в том числе СКЗИ и среда их функционирования.

3.5. С учетом имеющейся совокупности предположений о целях (мотивации) и возможностях нарушителей по реализации угроз безопасности персональных данных в ИСПДн потенциал нападения при реализации угроз безопасности персональных данных для рассматриваемых видов нарушителей будет 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 ограничена и контролируется организационными мерами и средствами ИСПДн.

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

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

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

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

несанкционированный физический доступ и (или) воздействие на объекты защиты (каналы (линии) связи, технические средства, носители информации).

4. Угрозы безопасности персональных данных, актуальные при их обработке 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. С учетом среднего уровня исходной защищенности ИСПДн, состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также особенностей их обработки для ИСПДн актуальны угрозы безопасности персональных данных третьего типа. Угрозы безопасности персональных данных третьего типа не связаны с наличием недокументированных (недекларированных) возможностей в используемом в ИСПДн системном и прикладном программном обеспечении.

4.3. Принимая во внимание природно-климатические условия, характерные для Брянской области в силу ее территориального положения, а также предпринятые операторами меры обеспечения безопасности персональных данных, приведенные в разделе 2 настоящих актуальных угроз, для ИСПДн техногенные угрозы, а также угрозы стихийных бедствий и иных природных явлений неактуальны, и далее будут рассматриваться только антропогенные (преднамеренные, непреднамеренные) угрозы безопасности персональных данных.

С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринятых операторами мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящих актуальных угроз, а также возможных негативных последствий (ущерба) от реализации, преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн неактуальны, и 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 принимаются угрозы, полученные из источников данных об угрозах безопасности информации, приведенных в пункте 1.7 настоящих актуальных угроз, реализуемые внутренними и внешними нарушителями с базовым (низким) потенциалом.

В качестве базового (предварительного) перечня угроз безопасности персональных данных для ИСПДн операторами рассматриваются угрозы, приведенные в приложении 1 к настоящим актуальным угрозам. При этом из базового (предварительного) перечня угроз безопасности персональных данных исключаются 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 актуальности угроз безопасности персональных данных из базового (предварительного) перечня для рассматриваемых типов ИСПДн осуществляется с учетом применения в них информационных технологий, необходимых для формирования соответствующих угроз, вероятности (частоты) их реализации, возможности реализации и опасности.

4.6. Вероятность (частота) реализации угроз безопасности персональных данных определяется экспертным путем и характеризуется вероятностью их реализации для ИСПДн с учетом реальных условий эксплуатации.

С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн вероятность (частота) реализации угроз безопасности персональных данных для ИСПДн оценивается не выше средней.

Экспертная оценка вероятности (частоты) реализации каждой угрозы безопасности персональных данных из базового (предварительного) перечня для рассматриваемых типов ИСПДн содержится в приложении 1 к настоящим актуальным угрозам.

Экспертная оценка вероятности (частоты) реализации угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн, осуществляется их операторами с учетом максимальных значений вероятности (частоты) реализации соответствующих угроз, приведенных в приложении 1 к настоящим актуальным угрозам, и приводится в частных моделях угроз, разрабатываемых для этих ИСПДн.

4.7. 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 уровня защищенности персональных данных в ИСПДн (необходимо обеспечение не выше чем второго уровня защищенности персональных данных) опасность угроз безопасности персональных данных для рассматриваемых типов ИСПДн оценивается не выше средней. В результате нарушения одного из свойств безопасности персональных данных (конфиденциальность, целостность, доступность) возможны умеренные негативные последствия для операторов и субъектов персональных данных.

Опасность угроз безопасности персональных данных, направленных на нарушение их целостности и доступности при обработке в ИСПДн с учетом предпринятых операторами мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящих актуальных угроз, оценивается как низкая. В результате нарушения одного из свойств безопасности персональных данных (целостность, доступность) возможны незначительные негативные последствия для операторов и субъектов персональных данных.

Экспертная оценка опасности каждой угрозы безопасности персональных данных из базового (предварительного) перечня для рассматриваемых типов ИСПДн содержится в приложении 1 к настоящим актуальным угрозам.

Оценка опасности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн, используется операторами из приложения 1 к настоящим актуальным угрозам и приводится в частных моделях угроз, разрабатываемых для этих ИСПДн.

4.8. Оценка возможности реализации и актуальности угроз безопасности персональных данных из базового (предварительного) перечня для рассматриваемых типов ИСПДн содержится в приложении 1 к настоящим актуальным угрозам.

Оценка возможности реализации и актуальности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн, осуществляется их операторами с учетом максимальных значений возможности реализации и актуальности соответствующих угроз, приведенных в приложении 1 к настоящим актуальным угрозам, и приводится в частных моделях угроз, разрабатываемых для этих ИСПДн.

4.9. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для рассматриваемых типов ИСПДн, в случае применения в них для обеспечения безопасности персональных данных СКЗИ, с учетом базового (низкого) потенциала возможных нарушителей и предпринятых операторами мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящих актуальных угроз, содержится в приложении 2 к настоящим актуальным угрозам.

Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн, в которых для обеспечения безопасности персональных данных операторами принято решение применения СКЗИ, используется операторами из приложения 2 к настоящим актуальным угрозам и приводится в частных моделях угроз, разрабатываемых для этих ИСПДн.

Приложение 1
к угрозам безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций

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

№ пп	Идентификатор угрозы из банка данных угроз	Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность реализации угрозы	Актуальность использования (применения) для построения и реализации атак
1.	УБИ.006[1]	угроза внедрения кода или данных	средняя	средняя	средняя	актуально
2.	УБИ.008	угроза восстановления аутентификационной информации	средняя	средняя	низкая	неактуально
3.	УБИ.014	угроза длительного удержания вычислительных ресурсов пользователями	маловероятная	низкая	низкая	неактуально
4.	УБИ.015	угроза доступа к защищаемым файлам с использованием обходного пути	средняя	средняя	средняя	актуально
5.	УБИ.017[1]	угроза доступа/перехвата/изменения HTTP cookies	маловероятная	низкая	средняя	неактуально
6.	УБИ.018	угроза загрузки нештатной операционной системы	низкая	средняя	средняя	актуально
7.	УБИ.019[1]	угроза заражения DNS-кеша	низкая	средняя	средняя	актуально
8.	УБИ.022	угроза избыточного выделения оперативной памяти	низкая	средняя	низкая	неактуально

№ пп	Идентификатор угрозы из банка данных угроз	Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность реализации угрозы	Актуальность использования (применения) для построения и реализации атак
9.	УБИ.027	угроза искажения вводимой и выводимой на периферийные устройства информации	маловероятная	низкая	низкая	неактуально
10.	УБИ.028	угроза использования альтернативных путей доступа к ресурсам	средняя	средняя	средняя	актуально
11.	УБИ.030	угроза использования информации идентификации/аутентификации, заданной по умолчанию	низкая	средняя	средняя	актуально
12.	УБИ.031	угроза использования механизмов авторизации для повышения привилегий	низкая	средняя	средняя	актуально
13.	УБИ.034[1]	угроза использования слабостей протоколов сетевого/локального обмена данными	средняя	средняя	средняя	актуально
14.	УБИ.041[1]	угроза межсайтового скриптинга	низкая	средняя	средняя	актуально
15.	УБИ.049	угроза нарушения целостности данных кэша	низкая	средняя	низкая	неактуально
16.	УБИ.051	угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	маловероятная	низкая	низкая	неактуально
17.	УБИ.062[1]	угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	низкая	средняя	средняя	актуально
18.	УБИ.067	угроза неправомерного ознакомления с защищаемой информацией	средняя	средняя	средняя	актуально
19.	УБИ.069[1]	угроза неправомерных действий в каналах связи	средняя	средняя	средняя	актуально
20.	УБИ.071	угроза несанкционированного восстановления удаленной защищаемой информации	низкая	средняя	средняя	актуально
21.	УБИ.074	угроза несанкционированного доступа к аутентификационной информации	низкая	средняя	средняя	актуально
22.	УБИ.084	угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	средняя	средняя	средняя	актуально

№ пп	Идентификатор угрозы из банка данных угроз	Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность реализации угрозы	Актуальность использования (применения) для построения и реализации атак
23.	УБИ.086	угроза несанкционированного изменения аутентификационной информации	низкая	средняя	низкая	неактуально
24.	УБИ.088	угроза несанкционированного копирования защищаемой информации	средняя	средняя	средняя	актуально
25.	УБИ.089	угроза несанкционированного редактирования реестра	средняя	средняя	средняя	актуально
26.	УБИ.090	угроза несанкционированного создания учетной записи пользователя	средняя	средняя	средняя	актуально
27.	УБИ.091	угроза несанкционированного удаления защищаемой информации	низкая	средняя	низкая	неактуально
28.	УБИ.093	угроза несанкционированного управления буфером	средняя	средняя	низкая	актуально
29.	УБИ.098[1]	угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	средняя	средняя	средняя	актуально
30.	УБИ.099[1]	угроза обнаружения хостов	средняя	средняя	средняя	актуально
31.	УБИ.100	угроза обхода некорректно настроенных механизмов аутентификации	маловероятная	средняя	низкая	неактуально
32.	УБИ.103[1]	угроза определения типов объектов защиты	низкая	средняя	низкая	неактуально
33.	УБИ.104[1]	угроза определения топологии вычислительной сети	средняя	средняя	низкая	неактуально
34.	УБИ.113	угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	средняя	средняя	низкая	неактуально
35.	УБИ.115	угроза перехвата вводимой и выводимой на периферийные устройства информации	низкая	средняя	средняя	актуально
36.	УБИ.116[1]	угроза перехвата данных, передаваемых по вычислительной сети	средняя	средняя	средняя	актуально
37.	УБИ.121	угроза повреждения системного реестра	низкая	низкая	низкая	неактуально

№ пп	Идентификатор угрозы из банка данных угроз	Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность реализации угрозы	Актуальность использования (применения) для построения и реализации атак
38.	УБИ.124	угроза подделки записей журнала регистрации событий	маловероятная	низкая	низкая	неактуально
39.	УБИ.128[1]	угроза подмены доверенного пользователя	низкая	средняя	средняя	актуально
40.	УБИ.130[1]	угроза подмены содержимого сетевых ресурсов	маловероятная	низкая	средняя	неактуально
41.	УБИ.140	угроза приведения системы в состояние «отказ в обслуживании»	средняя	средняя	низкая	неактуально
42.	УБИ.145	угроза пропуска проверки целостности программного обеспечения	маловероятная	низкая	низкая	неактуально
43.	УБИ.152	угроза удаления аутентификационной информации	низкая	средняя	низкая	неактуально
44.	УБИ.153	угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	низкая	средняя	низкая	неактуально
45.	УБИ.155	угроза утраты вычислительных ресурсов	низкая	средняя	низкая	неактуально
46.	УБИ.156	угроза утраты носителей информации	низкая	средняя	средняя	актуально
47.	УБИ.157[1]	угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	низкая	средняя	низкая	неактуально
48.	УБИ.158	угроза форматирования носителей информации	маловероятная	низкая	низкая	неактуально
49.	УБИ.159[1]	угроза «форсированного веб-браузинга»	низкая	средняя	средняя	актуально
50.	УБИ.160[1]	угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	маловероятная	низкая	средняя	неактуально
51.	УБИ.162	угроза эксплуатации цифровой подписи программного кода	маловероятная	низкая	низкая	неактуально
52.	УБИ.167[1]	угроза заражения компьютера при посещении неблагонадежных сайтов	средняя	средняя	средняя	актуально
53.	УБИ.168[1]	угроза «кражи» учетной записи доступа к сетевым сервисам	низкая	средняя	средняя	актуально

№ пп	Идентификатор угрозы из банка данных угроз	Наименование угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность реализации угрозы	Актуальность использования (применения) для построения и реализации атак
54.	УБИ.170[1]	угроза неправомерного шифрования информации	низкая	средняя	низкая	неактуально
55.	УБИ.171[1]	угроза скрытного включения вычислительного устройства в состав бот-сети	низкая	средняя	низкая	неактуально
56.	УБИ.172[1]	угроза распространения «почтовых червей»	средняя	средняя	средняя	актуально
57.	УБИ.174[1]	угроза «фарминга»	низкая	средняя	средняя	актуально
58.	УБИ.175[1]	угроза «фишинга»	средняя	средняя	средняя	актуально
59.	УБИ.176[1]	угроза нарушения технологического/ производственного процесса из-за временных задержек, вносимых средством защиты	маловероятная	низкая	низкая	неактуально
60.	УБИ.178	угроза несанкционированного использования системных и сетевых утилит	средняя	средняя	средняя	актуально
61.	УБИ.179	угроза несанкционированной модификации защищаемой информации	средняя	средняя	низкая	неактуально
62.	УБИ.185	угроза несанкционированного изменения параметров настройки средств защиты информации	маловероятная	низкая	средняя	неактуально
63.	УБИ.186[1]	угроза внедрения вредоносного кода через рекламу, сервисы и контент	средняя	средняя	низкая	неактуально
64.	УБИ.191	угроза внедрения вредоносного кода в дистрибутив программного обеспечения	низкая	средняя	средняя	актуально
65.	УБИ.192	угроза использования уязвимых версий программного обеспечения	средняя	средняя	средняя	актуально

[1]Угроза безопасности персональных данных рассматривается только для ИСПДн типов 2, 4 и 6 (в соответствии с пунктом 2.5 актуальных угроз).

Приложение 2
к угрозам безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Брянской области и подведомственных им организаций

Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн, в которых для обеспечения безопасности персональных данных принято решение применения СКЗИ

№ пп	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1	2	3	4
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	актуально	
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования; помещения, в которых находятся компоненты 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 дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих 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

1	2	3	4
			возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты. 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
1.3.	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	актуально	
1.4.	Использование штатных средств ИСПДн, в которой используется СКЗИ, ограниченное реализованными в ИСПДн мерами, направленными на предотвращение и пресечение несанкционированных действий	актуально	
2.1.	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 дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения

1	2	3	4
			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
2.2.	Возможность располагать или воздействовать на аппаратные компоненты СКЗИ и среду функционирования, 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 дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих 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
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среды функционирования, 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 третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении

1	2	3	4
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченных 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
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среды функционирования, в том числе с использованием исходных текстов входящего в среды 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
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного 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 третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении
4.2.	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
4.3.	Возможность располагать или воздействовать на любые компоненты СКЗИ и среду функционирования	неактуально	не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы