Приложение к
постановлению
правительства
Воронежской области
от 02 ноября 2017 г. № 869

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

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных правительства Воронежской области, исполнительных органов государственной власти Воронежской области и подведомственных им организаций (далее – Актуальные угрозы), определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Под 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 (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных).

Для информационных систем персональных данных правительства Воронежской области, исполнительных органов государственной власти Воронежской области и подведомственных им организаций (далее – ИСПДн) целью защиты информации является обеспечение 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 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, не преднамеренные 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.

1.4. 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 дополнительно 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.

1.5. Настоящие Актуальные угрозы также распространяются на государственные информационные системы (далее – ГИС) Воронежской области, в которых осуществляется обработка персональных данных. Такие ГИС Воронежской области в рамках настоящего документа будут рассматриваться как ИСПДн.

В случае если в ГИС Воронежской области кроме персональных данных обрабатывается иная информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, то для определения угроз безопасности такой информации и разработки моделей угроз безопасности информации кроме настоящих Актуальных угроз должны дополнительно применяться нормативные правовые и методические документы ФСТЭК России и ФСБ России.

1.6. Актуальные угрозы разработаны с использованием следующих документов:

Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ

«Об информации, информационных технологиях и о защите информации»;

постановления 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»;

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

постановления правительства Воронежской области от 18.11.2014 № 1024-ДСП «Об утверждении концепции защиты информации в Воронежской области»;

базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008 (далее – Базовая модель угроз);

методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;

методических рекомендаций 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, утвержденных руководством 8-го Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

1.7. Настоящие Актуальные угрозы, а также угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, 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).

1.8. Источником данных об угрозах безопасности информации, на основе которых определяются Актуальные угрозы, являются:

банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru, далее – Банк данных угроз);

Базовая модель угроз.

В качестве источника данных об угрозах безопасности информации, актуальных при обработке персональных данных в ИСПДн, используются настоящие Актуальные угрозы.

1.9. Определение угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, осуществляется правительством Воронежской области, исполнительными органами государственной власти Воронежской области и подведомственными им

организациями соответственно, в случае если они являются операторами ИСПДн.

В правительстве Воронежской области, исполнительных органах государственной власти Воронежской области и подведомственных им организациях актом руководителя утверждается перечень ИСПДн, операторами которых они являются (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.

1.10. В случае если Оператором в соответствии с пунктом 2.12 настоящих Актуальных угроз 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.

1.11. 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.

1.12. 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).

1.13. В целях снижения субъективных факторов при оценке угроз безопасности персональных данных в ИСПДн и разработки Частных моделей угроз Операторам рекомендуется привлекать нескольких сотрудников из разных подразделений (ответственных за обеспечение безопасности персональных данных, администраторов безопасности информации, системных администраторов и т.д.).

1.14. В рамках одной Частной модели угроз Операторам рекомендуется рассматривать угрозы безопасности персональных данных только для одной ИСПДн.

1.15. 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.

1.16. 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.

1.17. При необходимости для определения угроз безопасности персональных данных, актуальных при обработки 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.

1.18. 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.

Исключение составляют только Частные модели угроз, разрабатываемые для вновь создаваемых ГИС Воронежской области, которые в соответствии с пунктом 3 требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 06.07.2015 № 676, согласуются с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации.

1.19. 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, в следствии 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 в соответствии с пунктом 4.4 настоящих Актуальных угроз;

при повышении возможности реализации существующих угроз

безопасности персональных данных;

в иных случаях по решению Оператора.

2. Описание информационных систем персональных данных и особенностей их функционирования

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 подключение (незащищенное, защищенное) 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);

автоматизированные рабочие места, 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 подключение 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. Все 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.

Контролируемый доступ (контролируемая зона) в административные здания и (или) помещения обеспечивается, в том числе с использованием систем видеонаблюдения. Неконтролируемый вынос за пределы административных зданий технических средств ИСПДн запрещен.

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. Обеспечение антивирусного контроля в ИСПДн осуществляется в соответствии с установленным Операторами порядком с применением средств антивирусной защиты информации.

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 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 Интернет), 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 07.07.2003 № 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.

2.13. 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.

2.14. 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.

2.15. 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.

2.16. 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.

2.17. 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. 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. 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 Воронежской 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. В качестве базового (предварительного) перечня угроз безопасности персональных данных для рассматриваемых типов ИСПДн принимаются угрозы, полученные из источников данных об угрозах безопасности информации, приведенных в пункте 1.8 настоящих Актуальных угроз, и реализуемые внутренним и внешним нарушителем с базовым (низким) потенциалом. При этом из базового (предварительного) перечня угроз безопасности персональных данных исключаются угрозы безопасности информации, необходимые информационные технологии для формирования которых в рассматриваемых типах ИСПДн не применяются (не используются) в соответствии с пунктом 2.4 настоящих Актуальных угроз.

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 информации, необходимые информационные технологии или структурно-функциональные характеристики для формирования которых в ИСПДн не применяются (не используются) в соответствии с пунктом 2.4 настоящих Актуальных угроз и имеющие соответствующую пометку в приложении № 1 к настоящим Актуальным угрозам.

В случае если угроза безопасности персональных данных имеет несколько пометок в приложении № 1 к настоящим Актуальным угрозам, указывающих на необходимость наличия для ее формирования соответствующих информационных технологий или структурно-функциональных характеристик, то Оператором при принятии решения о включении (исключении) соответствующей угрозы из базового (предварительного) перечня угроз безопасности персональных данных для ИСПДн должна приниматься во внимание каждая из таких пометок.

Базовый (предварительный) перечень рассматриваемых угроз безопасности персональных данных для ИСПДн приводится в разрабатываемой для этой 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. Объективные предпосылки для реализации угроз безопасности персональных данных существуют, но принятые меры обеспечения безопасности персональных данных в ИСПДн недостаточны.

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 привлечением сотрудников, указанных в пункте 1.13 настоящих Актуальных угроз) 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 привлечением сотрудников, указанных в пункте 1.13 настоящих Актуальных угроз) 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 правительства Воронежской области, исполнительных органов государственной власти Воронежской области и подведомственных им организаций

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

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
2.	УБИ.006[1]	Угроза внедрения кода или данных	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
3.	УБИ.008	Угроза восстановления аутентификационной информации	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
4.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
5.	УБИ.011[2]	Угроза деавторизации санкционированного клиента беспроводной сети	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
6.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
7.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
8.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
9.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
10.	УБИ.017[1]	Угроза доступа/перехвата/изменения HTTP cookies	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы

[1] Угроза безопасности персональных данных рассматривается только для ИСПДн типов 2, 4 и 6.
[2] Угроза безопасности персональных данных рассматривается только для ИСПДн, в которых применяются беспроводные сети связи.

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
11.	УБИ.018	Угроза загрузки нештатной операционной системы	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
12.	УБИ.019[1]	Угроза заражения DNS-кеша	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
13.	УБИ.022	Угроза избыточного выделения оперативной памяти	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
14.	УБИ.023	Угроза изменения компонентов системы	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
15.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
16.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
17.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
18.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
19.	УБИ.034[1]	Угроза использования слабостей протоколов сетевого/локального обмена данными	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
20.	УБИ.041[1]	Угроза межсайтового скриптинга	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
21.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
22.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
23.	УБИ.049	Угроза нарушения целостности данных кеша	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
24.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
25.	УБИ.052[1, 3]	Угроза невозможности миграции образов	Неактуально	Малая вероятность реализации угрозы. Низкая

[3] Угроза безопасности персональных данных рассматривается только для ИСПДн, в которых применяются технологии виртуализации.

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
		виртуальных машин из-за несовместимости аппаратного и программного обеспечения		возможность реализации угрозы. Низкая опасность угрозы
26.	УБИ.053	Угроза невозможности управления правами пользователей BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
27.	УБИ.058[3]	Угроза неконтролируемого роста числа виртуальных машин	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
28.	УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
29.	УБИ.062[1]	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
30.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
31.	УБИ.069[1]	Угроза неправомерных действий в каналах связи	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
32.	УБИ.071	Угроза несанкционированного восстановления удаленной защищаемой информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
33.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
34.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
35.	УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
36.	УБИ.078[3]	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
37.	УБИ.079[3]	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
38.	УБИ.083[1, 2]	Угроза несанкционированного доступа к системе по беспроводным каналам	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
39.	УБИ.084	Угроза несанкционированного доступа к	Актуально	Средняя вероятность реализации угрозы. Средняя

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
		системе хранения данных из виртуальной и (или) физической сети		возможность реализации угрозы. Средняя опасность угрозы
40.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
41.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
42.	УБИ.088	Угроза несанкционированного копирования защищаемой информации	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
43.	УБИ.089	Угроза несанкционированного редактирования реестра	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
44.	УБИ.090	Угроза несанкционированного создания учетной записи пользователя	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
45.	УБИ.091	Угроза несанкционированного удаления защищаемой информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
46.	УБИ.093	Угроза несанкционированного управления буфером	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
47.	УБИ.098[1]	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
48.	УБИ.099[1]	Угроза обнаружения хостов	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
49.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
50.	УБИ.103[1]	Угроза определения типов объектов защиты	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
51.	УБИ.104[1]	Угроза определения топологии вычислительной сети	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
52.	УБИ.108[3]	Угроза ошибки обновления гипервизора	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
53.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
54.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
55.	УБИ.116[1]	Угроза перехвата данных, передаваемых по вычислительной сети	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
56.	УБИ.121	Угроза повреждения системного реестра	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
57.	УБИ.123	Угроза подбора пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
58.	УБИ.124	Угроза подделки записей журнала регистрации событий	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
59.	УБИ.125[1, 2]	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
60.	УБИ.126[1, 2]	Угроза подмены беспроводного клиента или точки доступа	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
61.	УБИ.128[1]	Угроза подмены доверенного пользователя	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
62.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
63.	УБИ.130[1]	Угроза подмены содержимого сетевых ресурсов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
64.	УБИ.133[1, 2]	Угроза получения сведений о владельце беспроводного устройства	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
65.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
66.	УБИ.144	Угроза программного сброса пароля BIOS	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
67.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
68.	УБИ.151[1]	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
69.	УБИ.152	Угроза удаления аутентификационной информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
70.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
71.	УБИ.155	Угроза утраты вычислительных ресурсов	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
72.	УБИ.156	Угроза утраты носителей информации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность
73.	УБИ.157[1]	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
74.	УБИ.158	Угроза форматирования носителей информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
75.	УБИ.159[1]	Угроза «форсированного веб-браузинга»	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
76.	УБИ.160[1]	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
77.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
78.	УБИ.167[1]	Угроза заражения компьютера при посещении неблагонадежных сайтов	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
79.	УБИ.168[1]	Угроза «кражи» учетной записи доступа к сетевым сервисам	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
80.	УБИ.170[1]	Угроза неправомерного шифрования информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
81.	УБИ.171[1]	Угроза скрытного включения вычислительного устройства в состав бот-сети	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
82.	УБИ.172[1]	Угроза распространения «почтовых червей»	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
83.	УБИ.173[1]	Угроза «спама» веб-сервера	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
84.	УБИ.174[1]	Угроза «фарминга»	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
85.	УБИ.175[1]	Угроза «фишинга»	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
86.	УБИ.176[1]	Угроза нарушения технологического/производственного	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы

№ п/п	Идентификатор угрозы из Банка данных угроз	Наименование угрозы	Актуальность использования (применения) для построения и реализации атак	Примечание
		процесса из-за временных задержек, вносимых средством защиты		
87.	УБИ.177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
88.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
89.	УБИ.179	Угроза несанкционированной модификации защищаемой информации	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
90.	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
91.	УБИ.182	Угроза физического устаревания аппаратных компонентов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
92.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
93.	УБИ.186[1]	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
94.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
95.	УБИ.192	Угроза использования уязвимых версий программного обеспечения	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы

Приложение № 2
к угрозам безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных правительства Воронежской области, исполнительных органов государственной власти Воронежской 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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
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 возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты. Установлен порядок обеспечивающий сохранность документаций на СКЗИ, машинных носителей информации с комплектами

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			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 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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			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

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
3.2.	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
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 среды функционирования	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы