ПРАВИТЕЛЬСТВО ИВАНОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 08.04.2019 № 124-п
г. Иваново

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, операторами которых являются Правительство Ивановской области и исполнительные органы государственной власти Ивановской области

В соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях обеспечения единого подхода к определению угроз безопасности персональных данных Правительство Ивановской области **п о с т а н о в л я е т**:

Определить перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, операторами которых являются Правительство Ивановской области и исполнительные органы государственной власти Ивановской области (прилагается).

Губернатор
Ивановской области **С.С. Воскресенский**

Приложение к постановлению
Правительства Ивановской области
от 08.04.2019 № 124-п

П Е Р Е Ч Е Н Ь
угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, операторами которых являются Правительство Ивановской области и исполнительные органы государственной власти Ивановской области

1. Общие положения

1.1. Под угрозами безопасности персональных данных для целей настоящего Перечня понимается совокупность условий и факторов, создающих опасность несанкционированного (в том числе случайного) доступа к персональным данным, результатом которого могут стать нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

Целью защиты информации в информационных системах персональных данных, операторами которых являются Правительство Ивановской области и исполнительные органы государственной власти Ивановской области (далее – ИСПДн, оператор ИСПДн), является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

1.2. В качестве источников угроз безопасности персональных данных в ИСПДн могут выступать субъекты (физические и юридические лица) или явления (техногенные аварии, стихийные бедствия и т.п.). При этом источники угроз могут быть следующих типов:

антропогенные источники (антропогенные угрозы);

техногенные источники (техногенные угрозы);

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

1.3. Источниками антропогенных угроз безопасности персональных данных могут выступать:

лица, осуществляющие преднамеренные действия с целью доступа к персональным данным, содержащимся в ИСПДн, или нарушения функционирования ИСПДн 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.

1.4. Настоящий Перечень содержит актуальные угрозы безопасности персональных данных, которые могут быть реализованы в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки. К настоящему Перечню также прилагаются предположения о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн, в случае применения в них для обеспечения безопасности персональных данных средств криптографической защиты информации (далее - СКЗИ).

1.5. Перечень также содержит угрозы, актуальные для государственных информационных систем Ивановской области, в которых осуществляется обработка персональных данных. Такие системы в рамках настоящего документа будут рассматриваться как ИСПДн.

1.6. Настоящий Перечень содержит угрозы безопасности персональных данных, актуальность которых определена по результатам оценки 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 составлен настоящий Перечень, являются:

банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru, далее - Банк данных угроз);

базовая модель угроз безопасности персональных данных ФСТЭК России.

1.8. При разработке моделей угроз для ИСПДн использование настоящего Перечня обязательно.

1.9. Настоящий Перечень применяется на всех этапах создания, эксплуатации и выводе из эксплуатации ИСПДн.

1.10. Настоящий Перечень может быть дополнен оператором ИСПДн при необходимости определения угроз безопасности персональных данных для конкретной ИСПДн.

1.11. Настоящий Перечень подлежит пересмотру в случае:

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

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

изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей

функционирования ИСПДн, следствием которых стало возникновение новых актуальных угроз безопасности персональных данных;

повышения возможности реализации или опасности существующих угроз безопасности персональных данных;

при появлении сведений и фактов о новых возможностях нарушителей.

2. Описание информационных систем персональных данных

2.1. Настоящий Перечень содержит актуальные угрозы безопасности персональных данных, обрабатываемых в ИСПДн, эксплуатация которых связана с реализацией трудовых отношений, оказанием государственных услуг и (или) осуществлением государственных и иных функций.

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

2.3. Настоящий Перечень содержит актуальные угрозы безопасности персональных данных для ИСПДн, которым необходимо обеспечить уровень защищенности персональных данных не выше второго уровня.

2.4. В зависимости от структуры ИСПДн подразделяются на автоматизированные рабочие места, локальные информационные системы и распределенные информационные системы.

В зависимости от наличия подключений к сетям связи общего пользования, в том числе к сети Интернет, ИСПДн подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

В зависимости от режима обработки информации ИСПДн подразделяются на однопользовательские и многопользовательские.

В зависимости от разграничения прав доступа пользователей ИСПДн подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

2.5. В ИСПДн могут применяться технологии виртуализации, клиент-серверные технологии, виртуальные частные сети (VPN), беспроводные сети связи, удаленный доступ, веб-технологии, кластеризация, сегментирование, мобильные устройства.

2.6. 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. В случае использования в ИСПДн одной из указанных технологий оператор ИСПДн должен дополнить настоящий Перечень актуальными для данной технологии угрозами.

2.7. 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 ИСПДн, для которых угрозы из настоящего Перечня будут актуальны:

1) 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 т.п.), входящих в состав АРМ);

2) автоматизированные рабочие места, имеющие подключение к сетям связи, включая сети связи общего пользования и (или) сети Интернет;

3) 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) сети Интернет;

4) локальные ИСПДн (комплекс АРМ, объединенных в единую информационную систему в пределах одного здания), имеющие подключение к сетям связи общего пользования и (или) сети Интернет;

5) 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) сети Интернет;

6) 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) сети Интернет.

2.8. Все технические средства ИСПДн находятся в пределах Российской Федерации. Контролируемой зоной ИСПДн являются административные здания или отдельные помещения операторов ИСПДн. 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.

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

2.9. Помещения, в которых ведется обработка персональных данных (далее - Помещения), оснащены входными дверьми с замками. Операторами ИСПДн устанавливается 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 ИСПДн 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.

2.10. 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 т.п.) (далее - машинные носители).

Операторами ИСПДн устанавливается порядок, обеспечивающий сохранность используемых машинных носителей. Хранятся машинные носители только в Помещениях в условиях, препятствующих свободному доступу к ним посторонних лиц. Выдача машинных носителей осуществляется только сотрудникам, допущенным к обработке персональных данных.

2.11. В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных операторы ИСПДн осуществляют их резервирование в соответствии с установленным порядком с использованием машинных носителей. В наличии имеются комплекты восстановления на применяемое в ИСПДн системное и прикладное программное обеспечение, а также средства защиты информации.

Для ключевых элементов ИСПДн предусмотрены источники резервного электропитания, при необходимости применяются системы вентиляции и кондиционирования воздуха, а также средства пожарной сигнализации.

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

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 средства криптографической защиты информации (далее - СКЗИ) (при необходимости).

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 ИСПДн 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;

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;

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

3. Оценка возможностей нарушителей

3.1. Нарушителем является физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИСПДн.

3.2. В зависимости от возможности доступа в контролируемую зону и возможностей по доступу к обрабатываемым персональным данным и (или) к компонентам ИСПДн выделяются следующие типы нарушителей:

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.

3.3. Для ИСПДн, указанных в пункте 2.7 настоящего Перечня, типов 1, 3 и 5, учитывая их структурно-функциональные характеристики и особенности функционирования, состав и объем обрабатываемых данных, рассматриваются следующие виды нарушителей:

лица, имеющие доступ к компонентам ИСПДН (могут привлекаться для установки, наладки, обслуживания и иных видов работ) - внутренние нарушители;

лица, имеющие доступ в контролируемую зону (охрана, уборщики и т.д.) - внутренние нарушители;

пользователи ИСПДн - внутренние нарушители.

3.4. Для ИСПДн, указанных в пункте 2.7 настоящего Перечня, типов 2, 4 и 6, учитывая их структурно-функциональные характеристики и особенности функционирования, состав и объем обрабатываемых данных, рассматриваются следующие виды нарушителей:

преступные группы или отдельные злоумышленники - внешние нарушители;

лица, имеющие доступ к компонентам ИСПДн (могут привлекаться для установки, наладки, обслуживания и иных видов работ) - внутренние нарушители;

лица, имеющие доступ в контролируемую зону (охрана, уборщики и т.д.) - внутренние нарушители;

пользователи ИСПДн - внутренние нарушители;

бывшие сотрудники оператора или бывшие пользователи ИСПДн - внешние нарушители.

3.5. 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.

3.6. С учетом имеющихся предположений о возможностях нарушителей по реализации угроз безопасности персональных данных определен базовый (низкий) потенциал нарушителей при реализации угроз безопасности персональных данных для рассматриваемых ИСПДн.

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.

3.7. Нарушители с базовым (низким) потенциалом могут использовать следующие способы для реализации угроз безопасности персональных данных в ИСПДн:

несанкционированный доступ и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), аппаратные закладки в компонентах системы);

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. Оценка угроз безопасности персональных данных в ИСПДн

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 рассматриваемых ИСПДн актуальны угрозы безопасности персональных данных третьего типа. Угрозы безопасности персональных данных третьего типа не связаны с наличием недокументированных (не декларированных) возможностей в используемом в ИСПДн системном и прикладном программном обеспечении.

4.3. Учитывая природно-климатические условия, характерные для Ивановской области, а также предпринимаемые операторами ИСПДн меры обеспечения безопасности персональных данных, приведенные в разделе 2 настоящего Перечня, техногенные угрозы, а также угрозы стихийных бедствий и иных природных явлений неактуальны для ИСПДн, и далее будут рассматриваться только антропогенные

(преднамеренные, непреднамеренные) угрозы безопасности персональных данных.

4.4. С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринимаемых операторами ИСПДн мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящего Перечня, а также возможных негативных последствий (ущерба) от реализации преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн неактуальны. Далее из преднамеренных угроз безопасности персональных данных будут рассматриваться только угрозы, реализуемые за счет несанкционированного доступа.

4.5. В качестве базового перечня актуальных угроз безопасности персональных данных для рассматриваемых типов ИСПДн принимаются угрозы, полученные из источников данных об угрозах безопасности информации, приведенных в пункте 1.7 настоящего Перечня, и реализуемые внутренним и внешним нарушителем с базовым (низким) потенциалом. При этом в базовый перечень актуальных угроз безопасности персональных данных не включены угрозы безопасности информации, информационные технологии для формирования которых в рассматриваемых типах ИСПДн не применяются.

4.6. В качестве базового перечня актуальных угроз безопасности персональных данных для ИСПДн операторами ИСПДн рассматриваются угрозы, приведенные в разделе 5 настоящего Перечня.

4.7. Оценка актуальности угроз безопасности персональных данных из базового перечня актуальных угроз для рассматриваемых ИСПДн осуществляется с учетом применения в них информационных технологий, необходимых для формирования соответствующих угроз, вероятности их реализации, возможности реализации и опасности.

4.8. Вероятность реализации угроз безопасности персональных данных определяется экспертным путем с учетом реальных условий эксплуатации ИСПДн.

С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн вероятность реализации угроз безопасности персональных данных для ИСПДн оценивается не выше средней. Объективные предпосылки для реализации угроз безопасности персональных данных существуют, но компенсируются принимаемыми мерами обеспечения безопасности персональных данных в ИСПДн.

Экспертная оценка вероятности реализации каждой угрозы безопасности персональных данных из базового перечня для рассматриваемых ИСПДн содержится в разделе 5 настоящего Перечня.

4.9. Опасность угроз безопасности персональных данных определяется экспертным путем и характеризуется возможными негативными последствиями от их реализации для оператора ИСПДн и

субъектов персональных данных.

С учетом состава (категории) и объема обрабатываемых в ИСПДн персональных данных, а также уровня защищенности персональных данных в ИСПДн (не выше второго уровня защищенности) 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 ИСПДн и субъектов персональных данных.

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

4.10. Экспертная оценка опасности каждой угрозы безопасности персональных данных, возможности их реализации, а также актуальность угроз безопасности персональных данных для рассматриваемых типов ИСПДн содержится в разделе 5 настоящего Перечня.

4.11. Имеющиеся предположения о возможностях, которые могут использоваться при подготовке и проведении атак для рассматриваемых ИСПДн, в случае применения в них для обеспечения безопасности персональных данных СКЗИ, с учетом базового (низкого) потенциала возможных нарушителей и предпринимаемых операторами ИСПДн мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящего Перечня, содержится в приложении к настоящему Перечню.

5. Перечень актуальных угроз безопасности персональных данных

№	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 (только для типов 2, 4	Угроза внедрения кода или данных	Актуально	Низкая вероятность реализации угрозы. Средняя возможность

	и 6)			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 (только при применении беспроводных технологий связи)	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 (только для типов 2, 4 и 6)	Угроза доступа/перехвата/изменения HTTP cookies	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
11.	УБИ.018	Угроза загрузки нештатной операционной системы	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
12.	УБИ.019 (только для	Угроза заражения DNS-кеша	Актуально	Низкая вероятность реализации угрозы.

	типов 2, 4 и 6)			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 (только для типов 2, 4 и 6)	Угроза использования слабостей протоколов сетевого/локального обмена данными	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
20.	УБИ.041 (только для типов 2, 4 и 6)	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 кэша	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 (только для типов 2, 4 и 6 при применении технологий виртуализации)	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Неактуально	Малая вероятность реализации угрозы. Низкая 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 (только при применении технологий виртуализации)	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 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	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 (только при применении технологий виртуализации)	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 (только при применении технологий виртуализации)	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 (только для типов 2, 4 и 6 при применении технологий беспроводной связи)	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 системе хранения данных из виртуальной и (или) физической сети	Актуально	Средняя вероятность реализации угрозы. Средняя 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 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	Угроза определения типов объектов защиты	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
51.	УБИ.104 (только для типов 2, 4 и 6)	Угроза определения топологии вычислительной сети	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
52.	УБИ.108 (только	Угроза ошибки обновления гипервизора	Неактуально	Малая вероятность реализации угрозы.

	при применении технологий виртуализации)			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
55.	УБИ.116 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6 при применении беспроводных технологий связи)	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
60.	УБИ.126 (только для типов 2, 4 и 6 при применении беспроводных технологий связи)	Угроза подмены беспроводного клиента или точки доступа	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы

61.	УБИ.128 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	Угроза подмены содержимого сетевых ресурсов	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
64.	УБИ.133 (только для типов 2, 4 и 6 при применении беспроводных технологий связи)	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	Неакту Неактуально ально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
68.	УБИ.151 (только для типов 2, 4 и 6)	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
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 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	Угроза «форсированного веб-браузинга»	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
76.	УБИ.160 (только для типов 2, 4 и 6)	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 (только для типов 2, 4 и 6)	Угроза заражения компьютера при посещении неблагонадежных сайтов	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
79.	УБИ.168 (только для типов 2, 4 и 6)	Угроза «кражи» учетной записи доступа к сетевым сервисам	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
80.	УБИ.170 (только для типов 2, 4 и 6)	Угроза неправомерного шифрования информации	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
81.	УБИ.171 (только для типов 2, 4	Угроза скрытного включения вычислительного устройства в состав бот-сети	Неактуально	Низкая вероятность реализации угрозы. Средняя возможность

	и 6)			реализации угрозы. Низкая опасность угрозы
82.	УБИ.172 (только для типов 2, 4 и 6)	Угроза распространения «почтовых червей»	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
83.	УБИ.173 (только для типов 2, 4 и 6)	Угроза «спама» веб-сервера	Неактуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Низкая опасность угрозы
84.	УБИ.174 (только для типов 2, 4 и 6)	Угроза «фарминга»	Актуально	Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
85.	УБИ.175 (только для типов 2, 4 и 6)	Угроза «фишинга»	Актуально	Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы
86.	УБИ.176 (только для типов 2, 4 и 6)	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Неактуально	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Низкая опасность угрозы
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	Неактуаль-но	Малая вероятность реализации угрозы. Низкая возможность реализации угрозы. Средняя опасность угрозы
93.	УБИ.186 (только для типов 2, 4 и 6)	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Неактуаль-но	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 к Перечню угроз
безопасности персональных данных,
актуальных при обработке персональных
данных в информационных системах
персональных данных, операторами которых являются
Правительство Ивановской области и исполнительные органы
государственной власти Ивановской области

Предположения 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

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования для построения и реализации атак	Обоснование отсутствия
1.	Проведение атаки при нахождении в пределах контролируемой зоны	Актуально	
2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты среды функционирования; 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 документации на СКЗИ,

			машинных носителей информации с комплектами восстановления СКЗИ, носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и указанные носители хранятся в условиях, препятствующих свободному доступу к ним посторонних лиц
3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы ИСПДн; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИСПДн; сведений о мерах по разграничению доступа в помещения, в которых находятся компоненты ИСПДн, на которых реализованы СКЗИ и среда функционирования	Актуально	
4.	Использование штатных средств ИСПДн, в которой используется СКЗИ, ограниченное реализованными в ИСПДн мерами, направленными на предотвращение и пресечение несанкционированных действий	Актуально	
5.	Физический доступ к компонентам ИСПДн, на которых реализованы СКЗИ и среда функционирования	Неактуально	Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн назначаются из числа доверенных лиц. Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн. Указанные помещения оснащены входными 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
6.	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 администрирования ИСПДн обладают только привилегированные пользователи
7.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов,	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности. Для ИСПДн актуальны угрозы

	сопровождающих функционирование СКЗИ и среды функционирования, и в области использования для реализации атак недокументированных (не декларированных) возможностей прикладного программного обеспечения		безопасности персональных данных третьего типа, не связанные с наличием недокументированных (не декларированных) возможностей в используемом системном и прикладном программном обеспечении
8.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИСПДн, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
9.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среду 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
10.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (не декларированных) 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 (не декларированных) возможностей в используемом системном и прикладном программном обеспечении

11.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования СКЗИ	Неактуально	Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности. Отсутствует в наличии конструкторская документация на аппаратные и программные компоненты среды функционирования СКЗИ
12.	Возможность 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