ГУБЕРНАТОР УЛЬЯНОВСКОЙ ОБЛАСТИ

У К А З

27 февраля 2018 г. №21

Экз. №_____

г. Ульяновск

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Правительстве Ульяновской области, исполнительных органах государственной власти Ульяновской области и подведомственных им организациях

В соответствии с частью 5 статьи 19 Федерального закона 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения единого подхода к определению угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Ульяновской области и подведомственных им организациях, п о с т а н о в л я ю:

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Правительстве Ульяновской области, исполнительных органах государственной власти Ульяновской области и подведомственных им организациях, согласно приложению к настоящему указу.

2. Рекомендовать органам местного самоуправления муниципальных образований Ульяновской области и подведомственным им организациям руководствоваться настоящим указом при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных.

Губернатор области С.И.Морозов

Ульяновская область Правительство

ПРИЛОЖЕНИЕ

к указу Губернатора
Ульяновской области
от 27 февраля 2018 г. № 21

УГРОЗЫ
безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Правительстве Ульяновской области, исполнительных органах государственной власти Ульяновской области и подведомственных им организациях

1. Общие положения

1.1. В настоящем документе рассматриваются угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в Правительстве Ульяновской области, исполнительных органах государственной власти Ульяновской области и подведомственных им организациях (далее – актуальные угрозы), которые определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Под актуальными угрозами понимается совокупность условий и факторов, создающих реальную опасность несанкционированного, в том числе случайного, доступа к персональным данным (далее также – ПДн) при их обработке в информационных системах персональных данных (далее также – ИСПДн) в Правительстве Ульяновской области, исполнительных органах государственной власти Ульяновской области (далее – государственные органы) и подведомственных им организациях, результатами которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия (нарушение конфиденциальности, целостности и доступности обрабатываемых ПДн).

1.3. Угрозы безопасности ПДн, обрабатываемых в ИСПДн государственных органов и подведомственных им организаций, относящиеся к актуальным угрозам, подлежат уточнению в ходе разработки операторами ИСПДн частных моделей угроз безопасности ПДн.

При разработке операторами ИСПДн частных моделей угроз безопасности ПДн проводится анализ структурно-функциональных характеристик конкретной ИСПДн, применяемых в ней информационных технологий и особенностей её функционирования. По результатам анализа оператор ИСПДн относит ИСПДн к одному из видов ИСПДн, приведённых в пункте 1.5 настоящего раздела.

В частной модели угроз безопасности ПДн указываются:

описание ИСПДн и её структурно-функциональных характеристик;

описание угроз безопасности ПДн с учётом совокупности факторов, которые могут использоваться при создании способов, подготовке и проведении несанкционированного доступа к ПДн, возможных уязвимостей ИСПДн, способов реализации угроз безопасности информации и последствий нарушения свойств безопасности информации.

Частная модель угроз безопасности ПДн разрабатывается оператором ИСПДн с учётом требований приказа Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа Федеральной службы безопасности Российской Федерации (далее – ФСБ России) от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости», а также банка данных угроз безопасности информации (http://bdu.fstec.ru).

1.4. Перечень актуальных угроз уточняется и дополняется Правительством Ульяновской области по мере выявления новых источников угроз, способов и средств реализации угроз безопасности ПДн в ИСПДн, согласуется с ФСТЭК России и ФСБ России в установленном порядке.

1.5. В государственных органах и подведомственных им организациях создаются и эксплуатируются информационные системы, в которых могут обрабатываться ПДн. В зависимости от предназначения такие информационные системы подразделяются на следующие:

ИСПДн обеспечения типовой деятельности;

ИСПДн обеспечения специальной деятельности.

1.5.1. ИСПДн обеспечения типовой деятельности – ИСПДн, предназначенные для автоматизации обеспечивающей деятельности государственных органов и подведомственных им организаций в рамках исполнения ими типовых полномочий, предусмотренных нормативными правовыми актами, за исключением специфических полномочий, автоматизация или информационная поддержка которых предусмотрена ИСПДн обеспечения специальной деятельности.

К ИСПДн обеспечения типовой деятельности относятся:

ИСПДн управления персоналом;

ИСПДн управления финансами;

ИСПДн документооборота;

ИСПДн информационного обеспечения;

ИСПДН иной деятельности.

1.5.2. ИСПДн обеспечения специальной деятельности – ИСПДн, предназначенные для автоматизации либо информационной поддержки предоставления государственных услуг и исполнения государственных функций, предусмотренных нормативными правовыми актами в качестве полномочий конкретного государственного органа. К ИСПДн обеспечения специальной деятельности относятся ИСПДн по направлениям деятельности государственных органов и подведомственных им организаций в рамках исполнения функций и (или) предоставления услуг (например: ИСПДн в сфере здравоохранения, образования, жилищно-коммунального хозяйства, социальной защиты и других).

2. ИСПДн обеспечения типовой деятельности

2.1. ИСПДн обеспечения типовой деятельности органов государственной власти и подведомственных им организаций характеризуется тем, что в качестве объектов информатизации выступают автономные автоматизированные рабочие места (далее – АРМ) или рабочие места локальных вычислительных сетей, имеющих или не имеющих подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод ПДн в ИСПДн осуществляется как с бумажных, так и с электронных носителей информации. ПДн субъектов могут выводиться из ИСПДн с целью передачи ПДн третьим лицам в предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» случаях как в электронном, так и в бумажном виде.

Операторами ИСПДн обеспечения типовой деятельности являются государственные органы и подведомственные им организации. Количество субъектов ПДн не превышает 100 тыс. единиц. ПДн хранятся на учтённых машинных носителях информации (далее – МНИ), в качестве которых используются средства электронно-вычислительной техники.

2.1.1. ИСПДн управления персоналом предназначены для персонального кадрового учёта, управления кадровым резервом, проведения аттестации, повышения квалификации и других целей, связанных с управлением персоналом.

В ИСПДн управления персоналом обрабатывается обязательный перечень информации, содержащей ПДн сотрудников, граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей государственной гражданской службы и о включении в кадровый резерв, а также граждан, претендующих на замещение должностей государственной гражданской службы, в том числе фамилия, имя, отчество, дата и место рождения, адрес, паспортные данные, сведения для заполнения личного дела, личные карточки сотрудников формы № Т-2, сведения из трудовой книжки, дополнительные сведения о сотрудниках.

2.1.2. ИСПДн управления финансами предназначены для обработки ПДн, необходимых для бухгалтерского и управленческого финансового учёта, предоставления информации в пенсионные и налоговые органы, системы обязательного медицинского страхования.

В ИСПДн управления финансами обрабатываются следующие сведения: фамилия, имя, отчество, дата и место рождения, паспортные данные, адрес, номер телефона, идентификационный номер налогоплательщика (далее – ИНН), страховой номер индивидуального лицевого счёта, табельный номер, должность, номер приказа и дата приёма на работу (увольнения), номер лицевого счёта для перечисления денежного содержания и иных выплат сотрудника государственного органа; фамилия, имя отчество, паспортные данные, адрес, должность, номер телефона (либо иной вид связи), ИНН, платёжные реквизиты граждан, являющихся стороной гражданско-правовых договоров.

2.1.3. ИСПДн документооборота предназначены для автоматизации делопроизводства, служебной переписки, архивной деятельности, учёта корреспонденции, обращений граждан, обеспечения доступа к электронным документам.

В ИСПДн документооборота обрабатываются следующие сведения: фамилия, имя, отчество, должность, контактные данные (адрес, электронный адрес, номер телефона) сотрудников государственного органа и подведомственных им организаций, а также граждан, иная информация, содержащая ПДн, в документах.

2.1.4. ИСПДн информационного обеспечения предназначена для автоматизации деятельности органов государственной власти и подведомственных им организаций.

В ИСПДн информационного обеспечения обрабатываются ПДн, содержащиеся в адресных и телефонных справочниках, иных базах данных, содержащих ПДн.

2.2. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных средств криптографической защиты информации (далее – СКЗИ).

Контролируемой зоной ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны ИСПДн находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны ИСПДн находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

2.3. В ИСПДн обеспечения типовой деятельности применяются следующие меры защиты ПДн и СКЗИ:

утверждение правил доступа в помещения, где располагаются АРМ, на которых осуществляется обработка ПДн, установлены СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждение перечня лиц, имеющих право доступа в помещения, где располагаются АРМ, на которых осуществляется обработка ПДн, установлены СКЗИ;

обеспечение доступа в контролируемую зону, где располагаются АРМ, на которых осуществляется обработка ПДн, установлены СКЗИ, в соответствии с контрольно-пропускным режимом;

нахождение в помещениях, где расположены АРМ, на которых осуществляется обработка ПДн, установлены СКЗИ, представителей технических, обслуживающих и других вспомогательных служб, а также сотрудников, не являющихся пользователями СКЗИ, только в присутствии уполномоченных сотрудников государственного органа;

информирование сотрудников, являющихся пользователями ИСПДн, но не являющихся пользователями СКЗИ, о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;

информирование пользователей СКЗИ о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;

оснащение помещений, в которых располагаются СКЗИ, входными дверьми с замками, обеспечение постоянного закрытия дверей таких помещений на замок и их открытия только для санкционированного прохода;

осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам;

осуществление регистрации и учёта действий пользователей ИСПДн с ПДн;

осуществление контроля целостности средств защиты информации;

использование на АРМ и серверах, на которых осуществляется обработка ПДн, установлены СКЗИ, сертифицированных средств защиты информации от несанкционированного доступа, сертифицированных средств антивирусной защиты.

2.4. ИСПДн управления персоналом может взаимодействовать с ИСПДн управления финансами.

3. ИСПДн обеспечения специальной деятельности

3.1. ИСПДн обеспечения специальной деятельности государственных органов и подведомственных им организаций характеризуется тем, что в качестве объектов информатизации выступают локальные или распределённые информационные системы областного масштаба, подключённые к сетям общего пользования и (или) сетям международного информационного обмена.

Ввод ПДн в ИСПДн осуществляется как с бумажных, так и с электронных носителей информации с целью предоставления государственных и муниципальных услуг либо исполнения государственных функций, ПДн могут выводиться из ИСПДн как в электронном, так и в бумажном виде.

Операторами ИСПДн обеспечения специальной деятельности являются государственные органы и подведомственные им организации. Количество субъектов ПДн превышает 100 тыс. единиц. ПДн хранятся на учтённых МНИ, в качестве которых используются средства электронно-вычислительной техники.

3.2. В ИСПДн обеспечения специальной деятельности обрабатываются ПДн, предоставляемые гражданами при обращении за получением государственных услуг. Для предоставления государственных услуг ПДн получаются из государственных информационных систем в соответствии с административными регламентами предоставления государственных услуг.

3.3. ИСПДн «Региональная система межведомственного электронного взаимодействия Ульяновской области» в соответствии с постановлением Правительства Ульяновской области от 26.06.2012 № 304-П «Об организации межведомственного информационного взаимодействия в электронной форме при предоставлении государственных и муниципальных услуг в Ульяновской области» предназначена для технологического обеспечения на территории Ульяновской области:

предоставления государственных и муниципальных услуг в электронной форме;

исполнения государственных и муниципальных функций в электронной форме;

межведомственного информационного взаимодействия в электронной форме.

3.4. ИСПДн областного государственного казённого учреждения «Корпорация развития интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области» (далее также – МФЦ) предназначена для обеспечения деятельности МФЦ на территории Ульяновской области в соответствии с постановлением Правительства Ульяновской области от 15.07.2013 № 298-П «Об утверждении перечня государственных услуг исполнительных органов государственной власти Ульяновской области, предоставление которых организуется в областном государственном казённом учреждении «Корпорация развития интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области».

В ИСПДн обрабатываются ПДн, предоставляемые гражданами при подаче заявления о предоставлении государственной услуги, получаемые из государственных информационных ресурсов, от государственных органов и учреждений и используемые для предоставления государственной услуги в соответствии с административными регламентами предоставления государственных и муниципальных услуг.

3.5. Информационный обмен по сетям связи общего пользования и (или) сетям международного информационного обмена осуществляется с использованием сертифицированных СКЗИ.

Контролируемой зоной ИСПДн являются здания или отдельные помещения, в которых расположены государственные органы и подведомственные им организации. В пределах контролируемой зоны ИСПДн находятся АРМ пользователей, серверы ИСПДн, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны ИСПДн находятся линии передачи данных и телекоммуникационное оборудование операторов связи, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3.6. В ИСПДн обеспечения специальной деятельности применяются меры по защите ПДн и СКЗИ, приведённые в пункте 2.3 раздела 2 настоящего документа.

4. Объекты защиты ИСПДн, классификация и характеристики нарушителей информационной безопасности

4.1. В системе защиты информации ИСПДн к объектам защиты относятся:

Объект 1 – ПДн;

Объект 2 – СКЗИ;

Объект 3 – среда функционирования СКЗИ (далее – СФ СКЗИ);

Объект 4 – информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

Объект 5 – документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн и её криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ СКЗИ;

Объект 6 – носители защищаемой информации, используемые в ИСПДн в процессе криптографической защиты ПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

Объект 7 – используемые в ИСПДн каналы (линии) связи, включая кабельные системы;

Объект 8 – общесистемное программное обеспечение (далее – ПО);

Объект 9 – прикладное ПО;

Объект 10 – специальное ПО;

Объект 11 – средства защиты информации;

Объект 12 – помещения, в которых находятся ресурсы ИСПДн, имеющие отношение к криптографической защите ПДн;

Объект 13 – средства вычислительной техники;

Объект 14 – МНИ;

Объект 15 – информационные технологии.

4.2. По наличию прав доступа и возможностей доступа к информации и (или) к компонентам ИСПДн нарушители информационной безопасности подразделяются на два типа:

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

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

4.3. Внешними нарушителями могут быть:

разведывательные службы государств;

криминальные структуры;

физические лица.

Внешний нарушитель имеет следующие возможности:

осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;

осуществлять несанкционированный доступ через АРМ, подключённые к сетям связи общего пользования и (или) сетям международного информационного обмена;

осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИСПДн.

4.4. Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

4.4.1. К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Лицо, относящееся к первой категории:

имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;

располагает фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;

располагает именами и может вести выявление паролей зарегистрированных пользователей;

изменяет конфигурацию технических средств ИСПДн, может вносить в неё программно-аппаратные закладки и обеспечивать съём информации, используя непосредственное подключение к техническим средствам ИСПДн.

4.4.2. Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Лицо, относящееся ко второй категории:

обладает всеми возможностями лиц первой категории;

знает по меньшей мере одно легальное имя доступа;

обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

4.4.3. К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удалённый доступ к ПДн по локальным и (или) распределённым информационным сетям.

Лицо, относящееся к третьей категории:

обладает всеми возможностями лиц первой и второй категорий;

располагает информацией о топологии ИСПДн на базе локальной и (или) распределённой информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн;

имеет возможность физического доступа к фрагментам технических средств ИСПДн.

4.4.4. К четвёртой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента ИСПДн.

Лицо, относящееся к четвёртой категории:

обладает всеми возможностями лиц предыдущих трёх категорий;

обладает полной информацией о системном и прикладном ПО, используемом в сегменте ИСПДн;

обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;

имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;

имеет доступ ко всем техническим средствам сегмента ИСПДн;

обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

4.4.5. К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Лицо, относящееся к пятой категории:

обладает всеми возможностями лиц предыдущих четырёх категорий;

обладает полной информацией о системном и прикладном ПО ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

4.4.6. К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Лицо, относящееся к шестой категории:

обладает всеми возможностями лиц предыдущих пяти категорий;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

не имеет прав доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

4.4.7. К седьмой категории относятся программисты-разработчики прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте.

Лицо, относящееся к седьмой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

обладает возможностями внесения ошибок, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

4.4.8. К восьмой категории относятся разработчики ИСПДн и лица, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн.

Лицо, относящееся к восьмой категории:

обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

4.5. Возможность или невозможность доступа нарушителей, относящихся к различным категориям, указанным в пункте 4.4 настоящего раздела, к объектам защиты ИСПДн определяется в соответствии с таблицей 1.

Таблица 1

	I категория	II категория	III категория	IV категория	V категория	VI категория	VII категория	VIII категория
1	2	3	4	5	6	7	8	9
Объект 1	нет доступа	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа	нет доступа
Объект 2	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	есть доступ
Объект 3	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	есть доступ
Объект 4	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 5	есть доступ	нет доступа	нет доступа	нет доступа	нет доступа	есть доступ	нет доступа	есть доступ
Объект 6	есть доступ	нет доступа	нет доступа	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 7	есть доступ	нет доступа	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа

1	2	3	4	5	6	7	8	9
Объект 8	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 9	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 10	нет доступа	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 11	нет доступа	нет доступа	нет доступа	есть доступ	есть доступ	есть доступ	нет доступа	нет доступа
Объект 12	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ
Объект 13	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ
Объект 14	нет доступа	нет доступа	нет доступа	нет доступа	нет доступа	нет доступа	нет доступа	есть доступ
Объект 15	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ	есть доступ

4.6. Источники атак на объекты ИСПДн располагают обобщёнными возможностями в соответствии с таблицей 2.

Таблица 2

№ п/п	Обобщённые возможности источников атак	Да/нет
1	2	3
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны ИСПДн	да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны ИСПДн, но без физического доступа к аппаратным средствам, на которых применяются СКЗИ и СФ СКЗИ	да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны ИСПДн с физическим доступом к	да

1	2	3
	аппаратным средствам, на которых применяются СКЗИ и СФ СКЗИ	
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области недокументированных возможностей прикладного ПО)	нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области недокументированных возможностей аппаратного и программного компонентов СФ СКЗИ)	нет

4.7. Уточнённые возможности нарушителей и направления атак приведены в таблице 3.

Таблица 3

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия актуальности использования (применения) для построения и реализации атак
1	2	3	4
1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ, и в области использования недокументированных (недекларированных) возможностей прикладного ПО	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя; высокая стоимость и сложность подготовки реализации возможности нарушителя
2.	Проведение лабораторных исследований СКЗИ, используемых	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных

1	2	3	4
	вне контролируемой зоны ИСПДн, ограниченное мерами, реализованными в ИСПДн, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		сведений, которые могут представлять интерес для реализации возможности нарушителя; высокая стоимость и сложность подготовки реализации возможности нарушителя
3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ СКЗИ, в том числе с использованием исходных текстов входящего в СФ СКЗИ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя; высокая стоимость и сложность подготовки реализации возможности нарушителя
4.	Создание способов, подготовка и проведение атак с привлечением специалистов в области недокументированных (недекларированных) возможностей системного ПО	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя; высокая стоимость и сложность подготовки реализации возможности нарушителя
5.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя

1	2	3	4
6.	Возможность воздействовать на любые компоненты СКЗИ и СФ СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя

5. Актуальные угрозы

5.1. Учитывая особенности обработки ПДн в государственных органах и подведомственных им организациях, а также категорию и объём ПДн, обрабатываемых в ИСПДн, основными характеристиками безопасности являются конфиденциальность, целостность и доступность ПДн.

Конфиденциальность ПДн – обязательное для соблюдения оператором или иным лицом, получившим доступ к ПДн, требование не допускать их распространение без согласия субъекта ПДн или наличия иного основания, предписанного законодательством Российской Федерации.

Целостность ПДн – состояние защищённости ПДн, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность ПДн при попытках несанкционированных воздействий на них в процессе обработки или хранения.

Доступность ПДн – состояние ПДн, при котором существует возможность получения и использования ПДн пользователями ИСПДн.

5.2. Угрозы безопасности ПДн, при обработке ПДн в ИСПДн подразделяются на угрозы первого, второго, третьего типа. Для определения актуальных угроз из общего перечня угроз безопасности выбираются только те угрозы, которые являются актуальными для ИСПДн в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 14 февраля 2008 года.

5.3. Основной целью применения СКЗИ в ИСПДн государственных органов и подведомственных им организациях является защита ПДн при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена, не защищённым от перехвата передаваемой по ним информации или от несанкционированных воздействий на эту информацию.

5.4. В ИСПДн обеспечения типовой и специальной деятельности государственных органов и подведомственных им организаций не используются отчуждаемые носители защищаемой информации, для которых несанкционированный доступ к хранимой на них информации не может быть исключён без использования криптографических методов и способов защиты информации.

5.5. Основными видами угроз безопасности ПДн в ИСПДн государственных органов и подведомственных им организаций являются:

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена (внешний нарушитель);

угрозы, возникновение которых напрямую зависит от свойств техники и ПО, используемого в ИСПДн;

угрозы, возникающие в результате внедрения аппаратных закладок и вредоносных программ;

угрозы, направленные на нарушение нормальной работы технических средств, используемых в ИСПДн;

угрозы, связанные с недостаточной квалификацией обслуживающего ИСПДн персонала.

5.6. Перечень актуальных и неактуальных угроз безопасности ИСПДн государственных органов и подведомственных им организаций приведён в таблице 4.

Таблица 4

№ п/п	Наименование угрозы безопасности	Актуальность	Обоснование отсутствия актуальности угроз безопасности
1	2	3	4
1.	Угрозы утечки по техническим каналам		
1.1.	Угрозы утечки акустической информации	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; не предусмотрено использование акустической информации при передаче конфиденциальной информации
1.2.	Угрозы утечки видовой информации	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности;

1	2	3	4
			высокая стоимость и сложность подготовки реализации возможности; применение организационных мер, исключающих утечку видовой информации (использование ширм, жалюзи, разворот мониторов в сторону от посетителей)
1.3.	Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности
2.	Угрозы несанкционированного доступа к информации		
2.1.	Угрозы уничтожения, хищения АРМ ИСПДн, носителей информации путём физического доступа к элементам ИСПДн		
2.1.1.	Кража персональной электронно-вычислительной машины (далее – ПЭВМ)	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; обеспечение доступа в контролируемую зону ИСПДн и помещения, где располагаются ПЭВМ, на которых установлены СКЗИ и СФ СКЗИ, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются компоненты СКЗИ и СФ СКЗИ, входными дверьми с замками

1	2	3	4
			(обеспечение постоянного закрытия дверей помещений на замок и их открытие только для санкционированного прохода); обеспечение нахождения представителей технических, обслуживающих и других вспомогательных служб и сотрудников, не являющихся пользователями СКЗИ, при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ СКЗИ, только в присутствии пользователей ИСПДн
2.1.2.	Кража носителей информации	Актуально	
2.1.3.	Кража ключей и атрибутов доступа	Актуально	
2.1.4.	Кража, модификация, уничтожение информации	Актуально	
2.1.5.	Вывод из строя узлов ПЭВМ, каналов связи	Актуально	
2.2.	Угрозы хищения, несанкционированной модификации или блокирования информации за счёт несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1.	Действия вредоносных программ (вирусов)	Актуально	

1	2	3	4
2.2.2.	Недекларированные возможности системного ПО и ПО для обработки ПДн	Определяет оператор ИСПДн	
2.2.3.	Установка ПО, не связанного с исполнением служебных обязанностей	Актуально	
2.2.4.	Сброс паролей, установленных в BIOS/ UEFI, без прохождения процедуры авторизации в системе	Актуально	
2.2.5.	Внедрение вредоносного кода в BIOS	Актуально	
2.2.6.	Неправомерное использование декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве ПЭВМ	Актуально	
2.2.7.	Неправомерное использование пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов	Актуально	
2.2.8.	Внедрение в BIOS/ UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи	Актуально	

1	2	3	4
2.2.9.	Использование нарушителем потенциально опасных возможностей BIOS/ UEFI	Актуально	
2.2.10.	Подбор пароля BIOS	Актуально	
2.2.11.	Восстановление предыдущей уязвимой версии BIOS	Актуально	
2.2.12.	Загрузка нештатной операционной системы	Актуально	
2.2.13.	Изменение режимов работы аппаратных элементов ПЭВМ	Актуально	
2.2.14.	Использование поддельных цифровых подписей BIOS	Актуально	
2.2.15.	Использование слабых криптографических алгоритмов BIOS	Актуально	
2.2.16.	Исчерпание запаса ключей, необходимых для обновления BIOS	Актуально	
2.2.17.	Нарушение изоляции среды исполнения BIOS	Актуально	
2.2.18.	Подмена резервной копии ПО BIOS	Актуально	
2.2.19.	Программный сброс пароля BIOS	Актуально	
2.2.20.	Сбой процесса обновления BIOS	Актуально	
2.2.21.	Установка уязвимых версий обновления ПО BIOS	Актуально	
2.2.22.	Подбор аутентификационной информации дискредитируемой учётной записи пользователя в системе	Актуально	

1	2	3	4
2.2.23.	Использование информации идентификации/аутентификации, заданной по умолчанию	Актуально	
2.2.24.	Извлечение паролей из оперативной памяти ПЭВМ или хищение файлов паролей с МНИ	Актуально	
2.2.25.	Неправомерный доступ к аутентификационной информации других пользователей системы с помощью штатных средств операционной системы или специальных программных средств	Актуально	
2.2.26.	Удаление из системы аутентификационной информации	Актуально	
2.2.27.	Обход некорректно настроенных механизмов аутентификации	Актуально	
2.2.28.	Несанкционированное изменение параметров настройки средств защиты информации	Актуально	
2.2.29.	Определение типов объектов защиты	Актуально	
2.2.30.	Несанкционированный доступ к программной среде управления средством защиты информации и изменение режима его функционирования	Актуально	

1	2	3	4
2.2.31.	Несанкционированное создание учётной записи пользователя	Актуально	
2.2.32.	Использование механизмов авторизации для повышения привилегий пользователя	Актуально	
2.2.33.	Несанкционированное использование учётной записи доступа к сетевым сервисам	Актуально	
2.2.34.	Хищение аутентификационной информации из временных файлов Cookie	Актуально	
2.2.35.	Скрытная регистрация вредоносной программой учётных записей администраторов системы	Актуально	
2.2.36.	Утечка пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Актуально	
2.3.	Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн в её составе из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппа-		

1	2	3	4
	ратуры из-за ненадёжности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
2.3.1.	Утрата ключей и атрибутов доступа	Актуально	
2.3.2.	Утрата носителей информации	Актуально	
2.3.3.	Непреднамеренная модификация (уничтожение) информации пользователями системы	Неактуально	Соблюдение требований инструкции пользователя, администратора безопасности; соблюдение технологического процесса обработки информации
2.3.4.	Утрата хранящейся на форматируемом носителе информации из-за случайного выполнения процедуры форматирования носителя информации	Неактуально	Соблюдение требований инструкции пользователя, администратора безопасности; соблюдение технологического процесса обработки информации
2.3.5.	Неправомерное ознакомление с защищаемой информацией	Актуально	
2.3.6.	Несанкционированное копирование защищаемой информации	Актуально	
2.3.7.	Непреднамеренное отключение средств защиты информации	Актуально	
2.3.8.	Выход из строя аппаратно-программных средств	Актуально	
2.3.9.	Несанкционированное редактирование реестра	Актуально	

1	2	3	4
2.3.10.	Сбой системы электроснабжения	Неактуально	Соблюдение правил эксплуатации технических средств; соблюдение технологического процесса обработки информации
2.3.11.	Стихийное бедствие	Неактуально	Низкая вероятность наступления для данной местности
2.4.	Угрозы преднамеренных действий внутренних нарушителей		
2.4.1.	Доступ к информации, модификация, уничтожение лицами, не допущенными к её обработке	Актуально	
2.4.2.	Разглашение информации, модификация, уничтожение пользователями системы, допущенными к её обработке	Актуально	
В случае подключения ИСПДн к локальным вычислительным сетям, имеющим подключения к сетям общего пользования и (или) сетям международного информационного обмена, дополнительно актуальными и неактуальными являются угрозы безопасности информации:			
2.5.	Угрозы несанкционированного доступа по каналам связи		
2.5.1.	Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Актуально	
2.5.2.	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих стан-	Актуально	

1	2	3	4
	ций ИСПДн, топологии сети, открытых портов и служб, открытых соединений		
2.5.3.	Угрозы выявления паролей по сети	Актуально	
2.5.4.	Угрозы навязывания ложного маршрута сети	Актуально	
2.5.5.	Угрозы подмены доверенного объекта в сети	Актуально	
2.5.6.	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Актуально	
2.5.7.	Угрозы типа «Отказ в обслуживании»	Актуально	
2.5.8.	Угрозы удалённого запуска приложений	Актуально	
2.5.9.	Угрозы внедрения по сети вредоносных программ	Актуально	
2.6.	Угрозы среды виртуализации		
2.6.1.	Совершение атаки с виртуальной машины на другую виртуальную машину	Актуально	
2.6.2.	Совершение атаки на систему управления виртуальной инфраструктурой	Актуально	
2.6.3.	Совершение атаки на монитор виртуальных машин из физической сети	Актуально	
2.6.4.	Нарушение процедуры аутентификации субъектов виртуализированного информационного взаимодействия	Актуально	

1	2	3	4
2.6.5.	Нарушение работоспособности информационных систем, построенных на основе технологии виртуализации, за счёт несанкционированного доступа к средствам виртуализации	Актуально	
2.6.6.	Атака на виртуальные каналы передачи данных	Актуально	
2.6.7.	Несанкционированный доступ к образам виртуальных машин	Актуально	
2.6.8.	Нарушение изоляции пользовательских данных внутри виртуальных машин	Актуально	
2.6.9.	Атака на гипервизор с виртуальной машины	Актуально	
2.6.10.	Атака на гипервизор из физической среды	Актуально	
2.6.11.	Атака на защищаемые виртуальные машины из физической сети	Актуально	
2.6.12.	Неконтролируемый рост числа виртуальных машин	Актуально	
2.6.13.	Атака на сеть репликации виртуальных машин	Актуально	
2.6.14.	Выход процесса за пределы виртуальной среды	Актуально	
В случае использования СКЗИ для защиты ПДн дополнительно актуальными и неактуальными являются угрозы безопасности информации:			
2.7.	Угрозы безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ		

1	2	3	4
2.7.1.	Подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ	Актуально	
2.7.2.	Подготовка и проведение атак на этапах жизненного цикла СКЗИ: разработка (модернизация) СКЗИ, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы): внесение несанкционированных изменений в СКЗИ, в СФ СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ СКЗИ	Неактуально	Приобретение дистрибутива СКЗИ, системного ПО и ПО для обработки ПДн у доверенной организации (лицензиата); использование на АРМ и серверах, на которых установлены СКЗИ, сертифицированных средств защиты информации от несанкционированного доступа, сертифицированных средств антивирусной защиты; соблюдение требований инструкции пользователя, администратора безопасности; соблюдение технологического процесса обработки информации; оснащение помещений, в которых располагаются компоненты СКЗИ и СФ СКЗИ, входными дверьми с замками (обеспечение постоянного закрытия дверей помещений на

1	2	3	4
			замок и их открытие только для санкционированного прохода); обеспечение нахождения представителей технических, обслуживающих и других вспомогательных служб и сотрудников, не являющихся пользователями СКЗИ, при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ СКЗИ, только в присутствии пользователей ИСПДн
2.7.3.	Проведение атаки нарушителем вне контролируемой зоны	Актуально	
2.7.4.	Проведение атак на этапе эксплуатации СКЗИ: на ПДн; на ключевую, аутентифицирующую и парольную информацию СКЗИ; на программные компоненты СКЗИ; на аппаратные компоненты СКЗИ; на программные компоненты СФ СКЗИ, включая ПО BIOS; на аппаратные компоненты СФ СКЗИ; на данные, передаваемые по каналам связи	Актуально	
2.7.5.	Получение из находящихся в свободном доступе источников (включая информационно-	Актуально	

1	2	3	4
	телекоммуникационные сети, доступ к которым не ограничен определённым кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об ИСПДн, в которой используются СКЗИ		
2.7.6.	Применение: находящихся в свободном доступе или используемых за пределами контролируемой зоны ИСПДн аппаратных средств и ПО, включая аппаратные и программные компоненты СКЗИ и СФ СКЗИ; специально разработанных аппаратных средств и ПО	Актуально	
2.7.7.	Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: каналов связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами; каналов распространения сигналов,	Актуально	

1	2	3	4
	сопровождающих функционирование СКЗИ и СФ СКЗИ		
2.7.8.	Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определённым кругом лиц, если системы, в которых используются СКЗИ, имеют выход в эти сети	Актуально	
2.7.9.	Использование на этапе эксплуатации находящихся за пределами контролируемой зоны системы аппаратных средств и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ	Актуально	
2.7.10.	Проведение атаки при нахождении в пределах контролируемой зоны системы	Неактуально	Проведение работ по подбору персонала; обеспечение доступа в контролируемую зону ИСПДн и помещения, где располагаются ПЭВМ, на которых установлены СКЗИ и СФ СКЗИ, в соответствии с контрольно-пропускным режимом; оснащение помещениий, в которых располагаются компоненты СКЗИ и СФ СКЗИ, входными дверьми с замками (обеспечение постоянного закрытия дверей помещений на

1	2	3	4
			замок и их открытие только для санкционированного прохода); обеспечение нахождения представителей технических, обслуживающих и других вспомогательных служб и сотрудников, не являющихся пользователями СКЗИ, при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ СКЗИ только в присутствии пользователей ИСПДн; осуществление разграничения и контроля доступа пользователей к защищаемым ресурсам; осуществление регистрации и учёта действий пользователей; использование на АРМ и серверах, на которых установлены СКЗИ: сертифицированных средств защиты информации от несанкционированного доступа; сертифицированных средств антивирусной защиты
2.7.11.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и СФ СКЗИ;	Неактуально	Проведение работ по подбору персонала; обеспечение доступа в контролируемую зону ИСПДн и помещения, где располагаются ПЭВМ, на которых установлены СКЗИ и СФ СКЗИ, в соответствии с контрольно-пропускным режимом;

1	2	3	4
	помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых установлены СКЗИ и СФ СКЗИ		оснащение помещений, в которых располагаются компоненты СКЗИ и СФ СКЗИ, входными дверьми с замками (обеспечение постоянного закрытия дверей помещений на замок и их открытие только для санкционированного прохода); обеспечение нахождения представителей технических, обслуживающих и других вспомогательных служб и сотрудников, не являющихся пользователями СКЗИ, при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ СКЗИ, только в присутствии пользователей ИСПДн; обеспечение доступа в контролируемую зону ИСПДн и помещения, где располагаются ПЭВМ, на которых установлены СКЗИ и СФ СКЗИ, в соответствии с контрольно-пропускным режимом; оснащение помещений, в которых располагаются компоненты СКЗИ и СФ СКЗИ, входными дверьми с замками (обеспечение постоянного закрытия дверей помещений на замок и их открытие только для санкционированного прохода)
2.7.12.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: сведений о физических мерах защиты	Актуально	

1	2	3	4
	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 ПЭВМ, на которых установлены СКЗИ и СФ СКЗИ		
2.7.13.	Использование штатных средств, ограниченное мерами, реализованными в ИСПДн, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Применение сертифицированных СКЗИ и средств защиты информации от несанкционированного доступа
2.7.14.	Использование физического доступа к средствам вычислительной техники, на которых установлены СКЗИ и СФ СКЗИ	Актуально	
2.7.15.	Возможность располагать аппаратными компонентами СКЗИ и СФ СКЗИ, ограниченная мерами, реализованными в ИСПДн, в которой используются СКЗИ, и направленными на предотвращение и	Актуально	

1	2	3	4
	пресечение несанкционированных действий		
2.7.16.	Проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя
2.7.17.	Проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя
2.7.18.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в системе, в которой используются СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя
2.7.19.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ СКЗИ, в том числе с	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя

1	2	3	4
	использованием исходных текстов входящего в СФ СКЗИ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		
2.7.20.	Проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя
2.7.21.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя
2.7.22.	Возможность располагать всеми аппаратными компонентами СКЗИ и СФ СКЗИ	Неактуально	Неосуществление обработки сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности нарушителя

5.7. Для определения актуальных угроз используются следующие основания:

1) определение типа угроз безопасности ПДн, актуальных для ИСПДн государственных органов и подведомственных им организаций, осуществляется оператором ПДн самостоятельно, с учётом оценки возможного вреда безопасности ПДн;

2) при создании ИСПДн государственные органы и подведомственные им организации руководствуются Положением о координации мероприятий по использованию информационно-коммуникационных технологий в деятельности исполнительных органов государственной власти Ульяновской области

и подведомственных им учреждений, утверждённым постановлением Правительства Ульяновской области от 28.02.2014 № 73-П «О координации мероприятий по использованию информационно-коммуникационных технологий, созданию, развитию, модернизации, эксплуатации информационных систем и информационно-телекоммуникационной инфраструктуры, осуществляемых исполнительными органами государственной власти Ульяновской области и подведомственными им учреждениями»;

3) использование единого подхода к созданию, развитию (модернизации) и эксплуатации государственных информационных систем Ульяновской области, основанного на согласовании технологий обработки информации с уполномоченной организацией по координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов и подведомственных им организаций;

4) реализация единого порядка согласования с уполномоченной организацией по координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов и подведомственных им организаций технических заданий и технических проектов на создание информационных систем.

5.8. ИСПДн обеспечения типовой деятельности государственных органов и подведомственных им организаций отличается следующими особенностями:

1) использованием стандартных (унифицированных) технических средств обработки информации;

2) использованием типового ПО;

3) наличием незначительного количества АРМ, участвующих в обработке ПДн;

4) дублированием информации, содержащей ПДн, на бумажных носителях и внешних накопителях информации;

5) незначительными негативными последствиями для субъектов ПДн при реализации угроз безопасности ИСПДн;

6) эксплуатацией ИСПДн (как правило) сотрудниками государственных органов и подведомственных им организаций без привлечения на постоянной основе сторонних организаций;

7) жёсткой регламентацией процедуры взаимодействия со сторонними организациями (банки, пенсионные, страховые и налоговые органы, органы статистики).

5.9. Актуальными угрозами ИСПДн обеспечения типовой деятельности государственных органов и подведомственных им организаций являются:

1) кража носителей информации;

2) кража ключей и атрибутов доступа;

3) вывод из строя узлов ПЭВМ, каналов связи;

4) нарушение ПО BIOS;

5) нарушение системы идентификации/аутентификации пользователей ИСПДн;

6) несанкционированное отключение средств защиты информации;

7) утрата ключей и атрибутов доступа к ИСПДн;

8) непреднамеренная модификация (уничтожение) информации пользователями;

9) непреднамеренное отключение средств защиты информации;

10) выход из строя аппаратно-программных средств;

11) разглашение информации, её модификация, уничтожение пользователями, допущенными к её обработке.

5.10. ИСПДн обеспечения специальной деятельности государственных органов и подведомственных им организаций отличается следующими особенностями:

1) использованием широкой номенклатуры (зачастую уникальных) технических средств получения, отображения и обработки информации;

2) использованием специального (адаптированного под конкретную задачу) ПО;

3) наличием значительного количества АРМ, участвующих в обработке ПДн;

4) построением ИСПДн на базе распределённой по территории Ульяновской области вычислительной сети со сложной архитектурой;

5) наличием выходов в сети общего пользования и (или) сети международного информационного обмена, локальные вычислительные сети сторонних организаций;

6) использованием разнообразной телекоммуникационной среды, принадлежащей различным операторам связи;

7) широким применением средств защиты информации, сертифицированных СКЗИ при информационном обмене по сетям связи общего пользования и (или) сетям международного информационного обмена;

8) использованием аутсорсинга при создании и эксплуатации ИСПДн и её элементов;

9) сложностью дублирования больших массивов информации, содержащей ПДн, на бумажных носителях и внешних накопителях информации;

10) значительными негативными последствиями при реализации угроз безопасности ИСПДн;

11) недостаточной квалификацией пользователей и обслуживающего ИСПДн и средства защиты информации персонала;

12) проблемами взаимодействия различных ИСПДн, вызванных несовершенством законодательства Российской Федерации и ведомственных инструкций.

5.11. Актуальными угрозами ИСПДн обеспечения специальной деятельности государственных органов и подведомственных им организаций являются:

1) кража носителей информации;

2) кража ключей и атрибутов доступа;

3) вывод из строя узлов ПЭВМ, каналов связи;

4) нарушение ПО BIOS;

5) нарушение системы идентификации/аутентификации пользователей ИСПДн;

6) несанкционированное отключение средств защиты информации;

7) утрата ключей и атрибутов доступа к ИСПДн;

8) непреднамеренная модификация (уничтожение) информации пользователями;

9) непреднамеренное отключение средств защиты информации;

10) выход из строя аппаратно-программных средств;

11) разглашение информации, её модификация, уничтожение пользователями, допущенными к её обработке;

12) угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

13) угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений;

14) угрозы выявления паролей по сети;

15) угрозы навязывания ложного маршрута сети;

16) угрозы подмены доверенного объекта в сети;

17) угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

18) угрозы типа «Отказ в обслуживании»;

19) угрозы удалённого запуска приложений;

20) угрозы внедрения по сети вредоносных программ;

21) совершение атаки с виртуальной машины на другую виртуальную машину;

22) совершение атаки на систему управления виртуальной инфраструктурой;

23) подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

24) проведение атаки нарушителем вне контролируемой зоны;

25) проведение атак на этапе эксплуатации СКЗИ:

а) на ПДн;

б) на ключевую, аутентифицирующую и парольную информацию СКЗИ;

в) на программные компоненты СКЗИ;

г) на аппаратные компоненты СКЗИ;

д) на программные компоненты СФ СКЗИ, включая ПО BIOS;

е) на аппаратные компоненты СФ СКЗИ;

ж) на данные, передаваемые по каналам связи;

26) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определённым кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об ИСПДн, в которой используются СКЗИ;

27) применение:

а) находящихся в свободном доступе или используемых за пределами контролируемой зоны ИСПДн аппаратных средств и ПО, включая аппаратные и программные компоненты СКЗИ и СФ СКЗИ;

б) специально разработанных аппаратных средств и ПО;

28) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:

а) каналов связи, не защищённых от несанкционированного доступа к информации организационными и техническими мерами;

б) каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ СКЗИ;

29) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определённым кругом лиц, если ИСПДн, в которых используются СКЗИ, имеют выход в эти сети;

30) использование на этапе эксплуатации находящихся за пределами контролируемой зоны аппаратных средств и ПО из состава средств ИСПДн, применяемых на местах эксплуатации СКЗИ.