МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ КАЛУЖСКОЙ ОБЛАСТИ

П Р И К А З

от 18 октября 2017 г. № 1213-п

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в министерстве экономического развития Калужской области

В соответствии с частью 5 статьи 19 Федерального закона «О персональных данных», постановлением Правительства Калужской области от 23.09.2016 № 511 «О министерстве экономического развития Калужской области» **ПРИКАЗЫВАЮ:**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в министерстве экономического развития Калужской области согласно приложению к настоящему приказу.

2. Рекомендовать руководителям подведомственных министерству экономического развития Калужской области организаций при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных, руководствоваться перечнем актуальных угроз, приведённых в приложении к настоящему приказу.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр
экономического развития
Калужской области **Д.О. Разумовский**

АДМИНИСТРАЦИЯ ГУБЕРНАТОРА КАЛУЖСКОЙ ОБЛАСТИ
Зарегистрировано в Государственном реестре правовых актов исполнительных органов государственной власти Калужской области
Регистрационный № 9066
от 30.10 2017 г.

Приложение к приказу
министерства экономического
развития Калужской области
от 18.10.2017 № 1213-п

УГРОЗЫ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, АКТУАЛЬНЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ КАЛУЖСКОЙ ОБЛАСТИ

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн) в министерстве экономического развития Калужской области (далее – министерство), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн в министерстве (далее – Актуальные угрозы безопасности ИСПДн) содержат перечень актуальных угроз безопасности персональных данных при их обработке в ИСПДн министерства, эксплуатируемых при осуществлении соответствующих видов деятельности.

1.3. При разработке Актуальных угроз безопасности ИСПДн использованы: «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена заместителем директора ФСТЭК России 14.02.2008), «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» (утверждена заместителем директора ФСТЭК России 15.02.2008), Банк данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены ФСБ России 31.03.2015 № 149/7/2/6-432), приказ 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 защищенности».

1.4. Актуальные угрозы безопасности ИСПДн уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

2. Виды деятельности министерства

В соответствии с Положением о министерстве, утвержденном постановлением Правительства Калужской области от 23.09.2016 № 511, в министерстве осуществляются следующие виды деятельности, при которых производится обработка персональных данных субъектов:

- обеспечение деятельности министерства;
- ведение бухгалтерского учета;
- ведение кадрового учёта, формирование кадрового резерва, представление к награждению;
- организация работы с обращениями граждан;
- оказание государственных услуг;
- ведение реестров, списков, перечней в соответствии с полномочиями министерства;
- исполнение иных функций, возложенных на министерство.

3. Описание используемых ИСПДн

3.1. При осуществлении соответствующих видов деятельности в министерстве создаются и эксплуатируются следующие информационные системы персональных данных:

1) информационная система управления персоналом. Предназначена для персонального кадрового учета, управления кадровым резервом, проведения аттестации, повышения квалификации и для других целей, связанных с управлением персоналом.

В информационной системе управления персоналом обрабатываются персональные данных государственных гражданских служащих и работников министерства; граждан, подавших сведения для участия в конкурсе на замещение вакантных должностей государственной гражданской службы Калужской области и на включение в кадровый резерв; а также граждан, претендующих на замещение должностей руководителей организаций, подведомственных министерству: фамилия, имя, отчество, дата и место рождения, адрес, паспортные данные, сведения для заполнения личного дела, сведения из трудовой книжки, дополнительный перечень информации, имеющей характер персональных данных работников.

2) информационная система управления финансами. Предназначена для обработки персональных данных, необходимых для бухгалтерского и управленческого финансового учета, предоставления информации в органы Пенсионного фонда Российской Федерации и налоговые органы, систему обязательного медицинского страхования.

В информационной системе управления финансами обрабатываются следующие персональные данные:

– персональные данные государственных гражданских служащих и работников министерства: фамилия, имя, отчество, дата и место рождения, паспортные данные, адрес, номер телефона, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, табельный номер, должность, номер приказа и дата поступления на государственную гражданскую службу (увольнения), номер приказа и дата принятия на работу (увольнения) работников, номер лицевого счета для перечисления денежного содержания и иных выплат гражданских служащих и работников;

– персональные данные физических лиц: фамилия, имя отчество, паспортные данные, адрес, должность, номер телефона (либо иной вид связи), идентификационный номер налогоплательщика, платежные реквизиты граждан, являющихся стороной государственного контракта (договора).

3) информационная система документооборота. Предназначена для автоматизации делопроизводства, служебной переписки, архивной деятельности, учета корреспонденции, обращений граждан, обеспечения доступа к электронным документам.

В информационной системе документооборота обрабатываются следующие персональные данные: фамилия, имя, отчество, должность, контактные данные (адрес, электронный адрес, номер телефона), иная информация, имеющая характер персональных данных.

4) информационные системы обеспечения специальной деятельности.

Информационные системы обеспечения специальной деятельности создаются и используются в следующих целях:

- подготовки доверенностей для физических лиц;
- ведения реестра государственной собственности Калужской области;
- возмещения части первоначального взноса по ипотечному кредитованию;
- оказания государственных услуг и исполнения иных функций в соответствии с полномочиями министерства.

Состав обрабатываемых персональных данных для каждой информационной системы обеспечения специальной деятельности определяется индивидуально в зависимости ее от назначения.

3.2. ИСПДн министерства имеют сходную структуру, однотипны и в зависимости от структуры относятся к одной из следующих категорий:

1) в качестве объектов информатизации выступают автономные автоматизированные рабочие места или рабочие места локальных ИСПДн, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;

2) в качестве объектов информатизации выступают автономные автоматизированные рабочие места или рабочие места локальных ИСПДн, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

3.3. Ввод персональных данных в ИСПДн и вывод данных из ИСПДн осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и компакт-диски.

3.4. В отдельных случаях при обработке персональных данных в ИСПДн могут применяться технологии виртуализации.

3.5. Доступ к ИСПДн ограничен перечнем государственных гражданских служащих и работников министерства.

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

3.7. Контролируемой зоной ИСПДн являются здания и отдельные помещения, в которых ведется обработка и хранение персональных данных. В

пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование информационных систем. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

3.8. В административных зданиях министерства осуществляется пропускной режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники исключено. Помещения оборудованы запирающимися дверями.

4. Характеристики безопасности информационных систем персональных данных

4.1. Учитывая особенности обработки персональных данных в министерстве, а также категорию и объем обрабатываемых в ИСПДн персональных данных, основными характеристиками безопасности информации ИСПДн являются конфиденциальность, целостность и доступность.

Конфиденциальность - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Целостность - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения.

Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

4.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия с персональными данными.

4.3. В зависимости от состава обрабатываемых персональных данных и типа актуальных угроз, необходимый уровень защищенности персональных данных для каждой ИСПДн определяется индивидуально.

4.4. Угрозы безопасности персональных данных, обрабатываемых в информационных системах персональных данных, приведенные в Актуальных угрозах безопасности ИСПДн, подлежат адаптации в ходе разработки частных моделей угроз безопасности персональных данных.

5. Применение средств криптографической защиты информации в информационных системах персональных данных

5.1. Актуальность применения в ИСПДн министерства СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном

обмене по сетям связи общего пользования и (или) сетям международного информационного обмена.

5.2. СКЗИ предназначены для защиты информации от действий со стороны лиц, не имеющих прав доступа к этой информации.

5.3. Принятыми организационно-техническими мерами в министерстве исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.

5.4. При эксплуатации СКЗИ соблюдаются требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

5.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

5.6. Объектами защиты в ИСПДн являются:

– персональные данные;

– средства криптографической защиты информации;

– среда функционирования СКЗИ (далее – СФ);

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

– документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

– носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые информационной системой каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

6. Определение возможностей создания способов, подготовки и проведения атак на объекты защиты

6.1. Реализация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, определяется возможностями источников атак:

– возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

– возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования;

– возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим

доступом к АС, на которых реализованы СКЗИ и среда их функционирования;

– 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);

– возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);

– возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).

Актуальной признана:

– возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны.

В Таблице № 1 приведены обоснования признания угроз, характерных для иных возможностей источников атак, неактуальными.

Таблица № 1

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	Проведение атаки при нахождении в пределах контролируемой зоны.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности

			информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения.

1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.
1.4	Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	проводятся работы по подбору персонала; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты.
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	не актуально	проводятся работы по подбору сотрудников; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются

			СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода.
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	проводятся работы по подбору сотрудников; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации.
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору сотрудников; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических,

			обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность

	(недекларированных) возможностей системного ПО.		подготовки реализации возможности; проводятся работы по подбору сотрудников; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

7. Определение актуальных угроз безопасности персональных данных в информационных системах персональных данных

7.1. Основными видами угроз безопасности персональных данных в ИСПДн являются:

1) угрозы утечки информации по техническим каналам:

1.1) угрозы утечки акустической (речевой) информации;

1.2) угрозы утечки видовой информации;

1.3) угрозы утечки информации по каналам побочного электромагнитного излучения и наводки;

2) угрозы несанкционированного доступа (далее - НСД) к информации:

2.1) угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

2.2) угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

2.3) угрозы внедрения вредоносных программ;

2.4) угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

- кража персональной электронной вычислительной машины (далее – ПЭВМ);
- кража носителей информации;
- кража ключей и атрибутов доступа;
- кража, модификация, уничтожение информации;
- вывод из строя узлов ПЭВМ, каналов связи;
- несанкционированное отключение средств защиты;

2.5) угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):

- действия вредоносных программ (вирусов);
- недекларированные возможности системного программного обеспечения и программного обеспечения для обработки персональных данных;
- установка программного обеспечения, не связанного с исполнением служебных обязанностей;

2.6) угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты персональных данных в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного характера (ударов молний, пожаров, наводнений и т.п.):

- утрата ключей и атрибутов доступа;
- непреднамеренная модификация (уничтожение) информации сотрудниками;

– непреднамеренное отключение средств защиты;
– выход из строя аппаратно-программных средств;
– сбой системы электроснабжения;
– стихийное бедствие;

2.7) угрозы преднамеренных действий внутренних нарушителей:

– доступ к информации, модификация, уничтожение информации лицами, не допущенными к ее обработке;
– разглашение информации, ее модификация или уничтожение сотрудниками, допущенными к ее обработке;

2.8) угрозы несанкционированного доступа по сети и каналам связи:

– угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации (перехват за пределами контролируемой зоны, перехват в пределах контролируемой зоны внешними нарушителями, перехват в пределах контролируемой зоны внутренними нарушителями);
– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
– угрозы выявления паролей по сети;
– угрозы навязывания ложного маршрута сети;
– угрозы подмены доверенного объекта в сети;
– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
– угрозы типа «Отказ в обслуживании»;
– угрозы удаленного запуска приложений;
– угрозы внедрения по сети вредоносных программ;

2.9) угрозы при использовании в ИСПДн технологии виртуализации:

– угрозы несанкционированного доступа к образам виртуальных машин;
– угрозы внедрения вредоносных программ в виртуальной машине.

3) Угрозы безопасности информации из состава Банка данных угроз безопасности информации (www.bdu.fstec.ru), потенциально опасные для информационных систем персональных данных:

УБИ.003: Угроза анализа криптографических алгоритмов и их реализации;
УБИ.007: Угроза воздействия на программы с высокими привилегиями;
УБИ.010: Угроза выхода процесса за пределы виртуальной машины;
УБИ.016: Угроза доступа к локальным файлам сервера при помощи URL;
УБИ.026: Угроза искажения XML-схемы;
УБИ.030: Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;
УБИ.033: Угроза использования слабостей кодирования входных данных;
УБИ.036: Угроза исследования механизмов работы программы;
УБИ.037: Угроза исследования приложения через отчёты об ошибках;
УБИ.042: Угроза межсайтовой подделки запроса;
УБИ.044: Угроза нарушения изоляции пользовательских данных внутри виртуальной машины;
УБИ.046: Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия;
УБИ.048: Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин;

УБИ.052: Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения;

УБИ.058: Угроза неконтролируемого роста числа виртуальных машин;

УБИ.063: Угроза некорректного использования функционала программного обеспечения;

УБИ.068: Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи;

УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;

УБИ.077: Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение;

УБИ.078: Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

УБИ.079: Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин;

УБИ.080: Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;

УБИ.084: Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети;

УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации;

УБИ.094: Угроза несанкционированного управления синхронизацией и состоянием;

УБИ.095: Угроза несанкционированного управления указателями;

УБИ.101: Угроза общедоступности облачной инфраструктуры;

УБИ.102: Угроза опосредованного управления группой программ через совместно используемые данные;

УБИ.108: Угроза ошибки обновления гипервизора;

УБИ.109: Угроза перебора всех настроек и параметров приложения;

УБИ.111: Угроза передачи данных по скрытым каналам;

УБИ.114: Угроза переполнения целочисленных переменных;

УБИ.117: Угроза перехвата привилегированного потока;

УБИ.118: Угроза перехвата привилегированного процесса;

УБИ.119: Угроза перехвата управления гипервизором;

УБИ.120: Угроза перехвата управления средой виртуализации;

УБИ.122: Угроза повышения привилегий;

УБИ.127: Угроза подмены действия пользователя путём обмана;

УБИ.131: Угроза подмены субъекта сетевого доступа;

УБИ.132: Угроза получения предварительной информации об объекте защиты;

УБИ.139: Угроза преодоления физической защиты;

УБИ.143: Угроза программного выведения из строя средств хранения,

обработки и (или) ввода/вывода/передачи информации;

УБИ.146: Угроза прямого обращения к памяти вычислительного поля суперкомпьютера;

УБИ.149: Угроза сбоя обработки специальным образом изменённых файлов;

УБИ.163: Угроза перехвата исключения/сигнала из привилегированного блока функций;

УБИ.170: Угроза неправомерного шифрования информации;

УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ.172: Угроза распространения «почтовых червей»;

УБИ.180: Угроза отказа подсистемы обеспечения температурного режима;

УБИ.181: Угроза перехвата одноразовых паролей в режиме реального времени;

УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент;

УБИ.187: Угроза несанкционированного воздействия на средство защиты информации;

УБИ.189: Угроза маскирования действий вредоносного кода;

УБИ.190: Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

УБИ.193: Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика.

7.2. Угрозами безопасности ПДн при их обработке в информационных системах с использованием СКЗИ являются:

1) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;

2) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ; к этапам жизненного цикла СКЗИ относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация;

3) проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона). Границей контролируемой зоны могут быть периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

4) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее - СФ), 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;

5) проведение атак на этапе эксплуатации СКЗИ на:

- персональные данные;

- ключевую, аутентифицирующую и парольную информацию СКЗИ;

- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;
- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;
- иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО);

6) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:

- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
- сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;
- содержание конструкторской документации на СКЗИ;
- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;
- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;
- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);
- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;
- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;
- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;
- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;

7) применение:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
- специально разработанных АС и ПО;

8) 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 защищенных от несанкционированного доступа к

информации организационными и техническими мерами;

- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

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

10) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства);

11) проведение атаки при нахождении в пределах контролируемой зоны;

12) проведение атак на этапе эксплуатации СКЗИ на следующие объекты:

- документацию на СКЗИ и компоненты СФ;

- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;

13) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

- сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;

14) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

15) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;

16) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

17) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;

18) проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ;

19) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;

20) возможность располагать всеми аппаратными компонентами СКЗИ и СФ.

7.3. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в министерстве:

угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных);

угрозы внедрения вредоносных программ;

утрата ключей и атрибутов доступа;

непреднамеренная модификация (уничтожение) информации сотрудниками;

угроза «Анализ сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации за пределами контролируемой зоны;

несанкционированный доступ через сети международного обмена;

несанкционированный доступ через локальную вычислительную сеть организации;

утечка атрибутов доступа;

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

угрозы выявления паролей по сети;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ;

угрозы несанкционированного доступа к образам виртуальных машин;

угрозы внедрения вредоносных программ в виртуальной машине.

Угрозы безопасности информации из состава Банка данных угроз безопасности информации (www.bdu.fstec.ru), актуальные для информационных систем персональных данных:

УБИ.003: Угроза анализа криптографических алгоритмов и их реализации;

УБИ.030: Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети;

УБИ.078: Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети;

УБИ.127: Угроза подмены действия пользователя путём обмана;

УБИ.170: Угроза неправомерного шифрования информации;

УБИ.171: Угроза скрытного включения вычислительного устройства в состав бот-сети;

УБИ.172: Угроза распространения «почтовых червей»;

УБИ.186: Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

7.4. Актуальные угрозы безопасности ПДн при их обработке в информационных системах персональных данных с использованием СКЗИ, определенные в соответствии с требованиями «Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при

осуществлении соответствующих видов деятельности» (утверждены ФСБ России 31.03.2015 № 149/7/2/6-432):

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

проведение атаки нарушителем вне КЗ;

проведение атак на этапе эксплуатации СКЗИ на:

- персональные данные;
- ключевую, аутентифицирующую и парольную информацию СКЗИ;
- программные компоненты СКЗИ;
- аппаратные компоненты СКЗИ;
- программные компоненты СФ, включая программное обеспечение BIOS;
- аппаратные компоненты СФ;
- данные, передаваемые по каналам связи;

получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть Интернет) информации об информационной системе, в которой используется СКЗИ;

применение:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
- специально разработанных АС и ПО;

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 защищенных от несанкционированного доступа к информации организационными и техническими мерами;
- каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;

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

использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ.