ПРИЛОЖЕНИЕ

УТВЕРЖДЕНЫ
постановлением администрации района
от 30.08.2023 № 747

УГРОЗЫ
безопасности персональные данных, актуальных при обработке персональных данных в информационных системах персональных данных, в администрации Первомайского района Тамбовской области и подведомственных ей организациях

1. Общие положения

1.1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в администрации Первомайского района Тамбовской области и в подведомственных ей организациях (далее - Актуальные угрозы безопасности ИСПДн), определены в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями от 6 февраля 2023г.), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изменениями и дополнениями от 28 мая 2019г.), приказом 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» (с изменениями и дополнениями от 14 мая 2020г.), приказом 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 защищенности», Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008, Методическими рекомендациями 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,

утверждёнными руководством 8-го Центра ФСБ России от 31.03.2015 №149/7/2/6-432, Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008, и Банком данных угроз безопасности информации, размещенным на официальном сайте ФСТЭК России (http://bdu.fstec.ru).

1.2. Актуальные угрозы безопасности ИСПДн содержат перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) администрации Первомайского района Тамбовской области и подведомственных ей организаций.

1.3. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки администрацией Первомайского района Тамбовской области и подведомственных ей организациях частных моделей угроз безопасности персональных данных для каждой информационной системы (далее - ИС).

1.4. При разработке частных моделей угроз безопасности персональных данных проводится анализ структурно-функциональных характеристик ИС, эксплуатируемой при осуществлении администрацией Первомайского района Тамбовской области и подведомственными ей организациями функций и полномочий, а также применяемых в них информационных технологий и особенностей ее функционирования, в том числе с использованием Банка данных угроз безопасности информации.

1.5. В частной модели угроз безопасности персональных данных указываются:

описание ИСПДн и ее структурно-функциональных характеристик;

описание угроз безопасности персональных данных с учетом совокупности предположений о способах, подготовке и проведении атак;

описание возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий нарушений безопасности информации.

1.6. Объектами информатизации в администрации Первомайского района Тамбовской области и подведомственных ей организаций выступают ИС, имеющие сходную структуру и одноточечное подключение к сетям общего пользования и (или) информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») через выделенную инфраструктуру - межведомственную сеть передачи данных Тамбовской области.

1.7. В зависимости от конкретного объекта информатизации ИС администрации Первомайского района Тамбовской области и подведомственных ей организаций делятся на два вида:

локальная ИС, рабочие места и базы данных которой расположены в пределах одного здания;

распределенная ИС, рабочие места которой расположены в пределах одного здания, а базы данных хранятся и обрабатываются в Центре обработки данных администрации области.

1.8. Базы данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение,

уточнение (обновление, изменение) персональных данных граждан Российской Федерации, находятся на территории Российской Федерации.

1.9. Ввод персональных данных в ИС и вывод данных из ИС осуществляются с использованием бумажных и электронных носителей информации. В качестве электронных носителей информации используются учтенные съемные носители информации и оптические диски. Доступ к ИСПДн ограничен перечнем муниципальных служащих или работников организаций, являющихся владельцем ИС.

1.10. Передача персональных данных в другие организации и в территориальные органы федеральных органов исполнительной власти по сетям общего пользования и (или) сети «Интернет» осуществляется с использованием сертифицированных шифровальных (криптографических) средств защиты информации (далее - СКЗИ).

1.11. Контролируемой зоной ИС являются административные здания администрации Первомайского района Тамбовской области и подведомственных ей организаций и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИС. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям общего пользования и (или) сети «Интернет».

1.12. В административных зданиях администрации Первомайского района Тамбовской области и подведомственных ей организаций:

должен быть организован пропускной режим;

должно быть исключено неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники;

помещения со средствами вычислительной техники должны быть оборудованы запирающимися дверями и опечатывающими устройствами;

дополнительно может быть организовано видеонаблюдение в коридорах, вестибюлях и холлах.

1.13. Защита персональных данных в ИС администрации Первомайского района Тамбовской области и подведомственных ей организациях и сетях общего пользования, подключаемых к сети «Интернет», обеспечивается средствами защиты информации (далее - СЗИ):

СЗИ от несанкционированного доступа, сертифицированными ФСТЭК России, не ниже 4 уровня контроля отсутствия недекларированных возможностей (далее - НДВ);

средствами антивирусной защиты, сертифицированными ФСТЭК России, не ниже 4 класса;

межсетевыми экранами, сертифицированными ФСТЭК России, не ниже 3 класса;

СКЗИ, формирующими виртуальные частные сети (VPN), сертифицированными ФСБ России по классу КС 1 и выше;

системами обнаружения вторжения не ниже 4 класса;

средством государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Характеристики безопасности информационных систем персональных данных:

2.1. Основными свойствами безопасности информации являются:

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

целостность - состояние защищенности информации, характеризуемое способностью ИС 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.

2.2. 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 ИС, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

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

2.4. Для ИСПДн администрации Первомайского района Тамбовской области и подведомственных ей организаций актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием НДВ в системном и прикладном программном обеспечении (далее - ПО), используемом в ИС.

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

3.1. Актуальность применения в ИСПДн администрации Первомайского района Тамбовской области и подведомственных ей организаций СКЗИ определяется необходимостью защиты персональных данных, в том числе при информационном обмене по сетям связи общего пользования и (или) сети «Интернет».

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

3.3. Принятыми организационно-техническими мерами в органах власти должна быть исключена возможность несанкционированного доступа потенциального нарушителя к ключевой информации СКЗИ.

3.4. При эксплуатации СКЗИ должны соблюдаться требования эксплуатационно-технической документации на СКЗИ и требования действующих нормативных правовых актов в области реализации и эксплуатации СКЗИ.

3.5. Для обеспечения безопасности персональных данных при их обработке в ИСПДн используются СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

3.6. 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, рабочие материалы и т. п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты среды функционирования СКЗИ;

носители защищаемой информации, используемые в ИС 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 ИС, имеющие отношение к криптографической защите персональных данных.

3.7. Реализация угроз безопасности персональных данных, обрабатываемых в ИСПДн, определяется возможностями источников атак. На основании исходных данных об объектах защиты и источниках атак в таблице 1 для администрации Первомайского района Тамбовской области и подведомственных ей организаций определены обобщенные возможности источников атак.

Таблица 1

Обобщенные возможности источников атак	Да/Нет
1	2
1. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2. 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	Да
3. 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	Нет
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 использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет

6. 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)	Нет

3.8 В соответствии с обобщенными возможностями источников атак (таблица 1) определены две актуальные уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы для ИС) (таблица 2).

Таблица 2

Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1	2	3
1. Проведение атаки при нахождении в пределах контролируемой зоны	Неактуально	Проводятся работы по подбору персонала; 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 надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется 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;

1	2	3
		осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные СЗИ от несанкционированного доступа (далее - НСД); используются сертифицированные средства антивирусной защиты
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 средств вычислительной техники (далее - СВТ) и СФ	Неактуально	Проводятся работы по подбору персонала; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с надежными замками, обеспечено постоянное закрытие дверей помещений на замок, и их открытие осуществляется только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения
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	Актуально	

1	2	3
4. Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	2 Актуально	3
5. Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Неактуально	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
6. 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	Неактуально	Проводятся работы по подбору персонала; 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
7. 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 НДВ прикладного ПО	Неактуально	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 персонала; 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;

1	2	3
		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 СЗИ от НСД; используются сертифицированные средства антивирусной защиты
8. 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	Неактуально	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
9. 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, непосред-ственно использующего вызовы программных функций СКЗИ	Неактуально	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
10. Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак НДВ системного ПО	Неактуально	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;

1	2	3
		проводятся работы по подбору персонала; 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 СЗИ от НСД; используются сертифицированные средства антивирусной защиты
11. Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
12. Возможность воздействовать на любые компоненты СКЗИ и СФ	Неактуально	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

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

4.1. На основе проведенного анализа банка данных угроз безопасности информации (www.bdu.fstec.ru) с учётом структурно-функциональных характеристик типовых ИС, а также применяемых в них информационных технологий и особенностей функционирования, в ИС администрации Первомайского района Тамбовской области и подведомственных ей учреждениях могут быть актуальны следующие угрозы безопасности ИСПДн:

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
ДОП.001	Угрозы, связанные с наличием недекларированных возможностей в системном программном обеспечении	Постановление Правительства № 1119
ДОП.002	Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО	Постановление Правительства № 1119
ДОП.003	Угрозы утечки информации по каналу побочных электромагнитных излучений и наводок	Базовая модель угроз
ДОП.004	Природные угрозы	Базовая модель угроз
ДОП.005	Техногенные угрозы	Базовая модель угроз
ДОП.006	Угроза утечки акустической (речевой) информации	Базовая модель угроз
ДОП.007	Угроза утечки видовой информации	Базовая модель угроз
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Банк данных угроз
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Банк данных угроз
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	Банк данных угроз
УБИ.004	Угроза аппаратного сброса пароля BIOS	Банк данных угроз
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Банк данных угроз
УБИ.006	Угроза внедрения кода или данных	Банк данных угроз
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Банк данных угроз
УБИ.008	Угроза восстановления аутентификационной информации	Банк данных угроз
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Банк данных угроз
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Банк данных угроз
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Банк данных угроз
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Банк данных угроз
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Банк данных угроз
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Банк данных угроз
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Банк данных угроз
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Банк данных угроз
УБИ.018	Угроза загрузки нештатной операционной системы	Банк данных угроз
УБИ.019	Угроза заражения DNS-кеша	Банк данных угроз
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Банк данных угроз
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Банк данных угроз
УБИ.022	Угроза избыточного выделения оперативной памяти	Банк данных угроз
УБИ.023	Угроза изменения компонентов системы	Банк данных угроз
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Банк данных угроз
УБИ.025	Угроза изменения системных и глобальных переменных	Банк данных угроз
УБИ.026	Угроза искажения XML-схемы	Банк данных угроз
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Банк данных угроз
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Банк данных угроз
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Банк данных угроз
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Банк данных угроз
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Банк данных угроз
УБИ.033	Угроза использования слабостей кодирования входных данных	Банк данных угроз
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Банк данных угроз
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Банк данных угроз
УБИ.036	Угроза исследования механизмов работы программы	Банк данных угроз
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Банк данных угроз
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Банк данных угроз
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Банк данных угроз
УБИ.040	Угроза конфликта юрисдикций различных стран	Банк данных угроз
УБИ.041	Угроза межсайтового скриптинга	Банк данных угроз
УБИ.042	Угроза межсайтовой подделки запроса	Банк данных угроз
УБИ.043	Угроза нарушения доступности облачного сервера	Банк данных угроз
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Банк данных угроз
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Банк данных угроз
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Банк данных угроз
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Банк данных угроз
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Банк данных угроз
УБИ.049	Угроза нарушения целостности данных кеша	Банк данных угроз
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Банк данных угроз
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Банк данных угроз
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Банк данных угроз
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Банк данных угроз
УБИ.055	Угроза незащищённого администрирования облачных услуг	Банк данных угроз
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Банк данных угроз
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Банк данных угроз
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Банк данных угроз
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Банк данных угроз
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Банк данных угроз
УБИ.061	Угроза некорректного задания структуры данных транзакции	Банк данных угроз
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Банк данных угроз
УБИ.063	Угроза некорректного использования функционала программного обеспечения	Банк данных угроз
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Банк данных угроз
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Банк данных угроз
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Банк данных угроз
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Банк данных угроз
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.069	Угроза неправомерных действий в каналах связи	Банк данных угроз
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Банк данных угроз
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Банк данных угроз
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Банк данных угроз
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Банк данных угроз
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Банк данных угроз
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Банк данных угроз
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Банк данных угроз
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Банк данных угроз
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Банк данных угроз
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Банк данных угроз
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Банк данных угроз
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Банк данных угроз
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Банк данных угроз
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Банк данных угроз
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Банк данных угроз
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Банк данных угроз
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Банк данных угроз
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Банк данных угроз
УБИ.089	Угроза несанкционированного редактирования реестра	Банк данных угроз
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Банк данных угроз
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Банк данных угроз
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Банк данных угроз
УБИ.093	Угроза несанкционированного управления буфером	Банк данных угроз
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Банк данных угроз
УБИ.095	Угроза несанкционированного управления указателями	Банк данных угроз
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Банк данных угроз
УБИ.097	Угроза несогласованности правил доступа к большим данным	Банк данных угроз
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Банк данных угроз
УБИ.099	Угроза обнаружения хостов	Банк данных угроз
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Банк данных угроз
УБИ.101	Угроза общедоступности облачной инфраструктуры	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Банк данных угроз
УБИ.103	Угроза определения типов объектов защиты	Банк данных угроз
УБИ.104	Угроза определения топологии вычислительной сети	Банк данных угроз
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Банк данных угроз
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Банк данных угроз
УБИ.107	Угроза отключения контрольных датчиков	Банк данных угроз
УБИ.108	Угроза ошибки обновления гипервизора	Банк данных угроз
УБИ.109	Угроза перебора всех настроек и параметров приложения	Банк данных угроз
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Банк данных угроз
УБИ.111	Угроза передачи данных по скрытым каналам	Банк данных угроз
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Банк данных угроз
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Банк данных угроз
УБИ.114	Угроза переполнения целочисленных переменных	Банк данных угроз
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Банк данных угроз
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Банк данных угроз
УБИ.117	Угроза перехвата привилегированного потока	Банк данных угроз
УБИ.118	Угроза перехвата привилегированного процесса	Банк данных угроз
УБИ.119	Угроза перехвата управления гипервизором	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.120	Угроза перехвата управления средой виртуализации	Банк данных угроз
УБИ.121	Угроза повреждения системного реестра	Банк данных угроз
УБИ.122	Угроза повышения привилегий	Банк данных угроз
УБИ.123	Угроза подбора пароля BIOS	Банк данных угроз
УБИ.124	Угроза подделки записей журнала регистрации событий	Банк данных угроз
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Банк данных угроз
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Банк данных угроз
УБИ.127	Угроза подмены действия пользователя путём обмана	Банк данных угроз
УБИ.128	Угроза подмены доверенного пользователя	Банк данных угроз
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Банк данных угроз
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Банк данных угроз
УБИ.131	Угроза подмены субъекта сетевого доступа	Банк данных угроз
УБИ.132	Угроза получения предварительной информации об объекте защиты	Банк данных угроз
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Банк данных угроз
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Банк данных угроз
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Банк данных угроз
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Банк данных угроз
УБИ.137	Угроза потери управления облачными ресурсами	Банк данных угроз
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Банк данных угроз
УБИ.139	Угроза преодоления физической защиты	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Банк данных угроз
УБИ.141	Угроза привязки к поставщику облачных услуг	Банк данных угроз
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Банк данных угроз
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз
УБИ.144	Угроза программного сброса пароля BIOS	Банк данных угроз
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Банк данных угроз
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Банк данных угроз
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Банк данных угроз
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Банк данных угроз
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Банк данных угроз
УБИ.150	Угроза сбоя процесса обновления BIOS	Банк данных угроз
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Банк данных угроз
УБИ.152	Угроза удаления аутентификационной информации	Банк данных угроз
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Банк данных угроз
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Банк данных угроз
УБИ.155	Угроза утраты вычислительных ресурсов	Банк данных угроз
УБИ.156	Угроза утраты носителей информации	Банк данных угроз
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.158	Угроза форматирования носителей информации	Банк данных угроз
УБИ.159	Угроза «форсированного веб-браузинга»	Банк данных угроз
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Банк данных угроз
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Банк данных угроз
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Банк данных угроз
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Банк данных угроз
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Банк данных угроз
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Банк данных угроз
УБИ.166	Угроза внедрения системной избыточности	Банк данных угроз
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Банк данных угроз
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Банк данных угроз
УБИ.169	Угроза наличия механизмов разработчика	Банк данных угроз
УБИ.170	Угроза неправомерного шифрования информации	Банк данных угроз
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Банк данных угроз
УБИ.172	Угроза распространения «почтовых червей»	Банк данных угроз
УБИ.173	Угроза «спама» веб-сервера	Банк данных угроз
УБИ.174	Угроза «фарминга»	Банк данных угроз
УБИ.175	Угроза «фишинга»	Банк данных угроз
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Банк данных угроз
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Банк данных угроз
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Банк данных угроз
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Банк данных угроз
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Банк данных угроз
УБИ.182	Угроза физического устаревания аппаратных компонентов	Банк данных угроз
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Банк данных угроз
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Банк данных угроз
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Банк данных угроз
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Банк данных угроз
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Банк данных угроз
УБИ.188	Угроза подмены программного обеспечения	Банк данных угроз
УБИ.189	Угроза маскирования действий вредоносного кода	Банк данных угроз
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Банк данных угроз
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Банк данных угроз
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Банк данных угроз
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Банк данных угроз
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Банк данных угроз
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Банк данных угроз
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Банк данных угроз
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Банк данных угроз
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Банк данных угроз
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Банк данных угроз
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Банк данных угроз
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Банк данных угроз
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Банк данных угроз
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Банк данных угроз
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Банк данных угроз
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Банк данных угроз
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Банк данных угроз
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Банк данных угроз
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Банк данных угроз
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечениям администрирования информационных систем	Банк данных угроз
УБИ.212	Угроза перехвата управления информационной системой	Банк данных угроз
УБИ.213	Угроза обхода многофакторной аутентификации	Банк данных угроз
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Банк данных угроз
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Банк данных угроз
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Банк данных угроз
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Банк данных угроз
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Банк данных угроз
УБИ.219	Угроза хищения обучающих данных	Банк данных угроз
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Банк данных угроз

Идентификатор УБИ	Наименование УБИ	Источник сведений об угрозе
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Банк данных угроз
УБИ.222	Угроза подмены модели машинного обучения	Банк данных угроз

4.2 Угрозами безопасности персональных данных при их обработке с использованием СКЗИ являются:

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

4.2.2. 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;

4.2.3. 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 может быть: периметр охраняемой территории организации, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

4.2.4. 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, в совокупности представляющие среду функционирования СКЗИ, которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;

4.2.5. 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;

4.2.6. 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 ИС, в которой используется СКЗИ. При этом может быть получена следующая информация:

общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС);

сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в ИС совместно с 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);

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

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

сведений о физических мерах защиты объектов, в которых размещены ресурсы ИС;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИС;

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

4.2.9 использование штатных средств, ограниченное мерами, реализованными в ИС, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.