



ИНСПЕКЦИЯ ГОСУДАРСТВЕННОГО ЖИЛИЩНОГО НАДЗОРА  
ВОЛГОГРАДСКОЙ ОБЛАСТИ  
(ГОСЖИЛНАДЗОР)

Приказ

26 декабря 2022 г.

№ 260

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности инспекции государственного жилищного надзора Волгоградской области

В соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных",

**п р и к а з ы в а ю:**

1. Определить:

перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности инспекции государственного жилищного надзора Волгоградской области, защищаемых с использованием средств криптографической защиты информации (далее – Перечень 1), согласно приложению 1 к настоящему приказу.

перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности инспекции государственного жилищного надзора Волгоградской области, защищаемых без использования средств криптографической защиты информации (далее – Перечень 2), согласно приложению 2 к настоящему приказу.

2. Ответственному за обеспечение безопасности персональных данных и защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах инспекции государственного жилищного надзора Волгоградской области определять угрозы безопасности персональных данных при их обработке в информационных системах исходя из Перечня 1 и Перечня 2 с учетом структурно-функциональных характеристик информационных систем.

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя – начальника инспекционного отдела инспекции государственного жилищного надзора Волгоградской области А.В. Говоруна.

4. Настоящий приказ вступает в силу со дня его подписания и подлежит официальному опубликованию.

Руководитель



С.В. Данилов

Приложение 1  
к приказу инспекции государственного  
жилищного надзора  
Волгоградской области  
от 26 декабря 2022 г. № 260

Перечень угроз безопасности персональных данных, актуальных  
при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности  
инспекции государственного жилищного надзора Волгоградской области, защищаемых  
с использованием средств криптографической защиты информации

Пункт приложения к приказу ФСБ России от 10 июля 2014 г. N 378 <*>	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности
подпункт "а" пункта 10	Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа средств криптографической защиты информации (далее - СКЗИ)	Актуально	
подпункт "б" пункта 10	Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ	Актуально	
подпункт "в" пункта 10	Проведение атаки, при нахождении вне контролируемой зоны (далее - КЗ)	Актуально	
подпункт "г" пункта 10	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	Неактуально	Работы проводят лицензиаты ФСБ России, не имеющие коммерческой выгоды в перехвате данных передаваемых по зашифрованным каналам связи

	<p>совокупности представляющие среду функционирования (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;</p> <ul style="list-style-type: none"> <li>- внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ</li> </ul>		
<p>подпункт "д" пункта 10</p>	<p>Проведение атак на этапе эксплуатации СКЗИ на:</p> <ul style="list-style-type: none"> <li>- персональные данные;</li> <li>- ключевую, аутентифицирующую и парольную информацию СКЗИ;</li> <li>- программные компоненты СКЗИ;</li> <li>- аппаратные компоненты СКЗИ;</li> <li>- программные компоненты СФ, включая программное обеспечение BIOS;</li> <li>- аппаратные компоненты СФ;</li> <li>- данные, передаваемые по каналам связи;</li> <li>- 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, информационных систем и системного программного обеспечения</li> </ul>	Актуально	
<p>подпункт "е" пункта 10</p>	<p>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:</p> <ul style="list-style-type: none"> <li>- общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав,</li> </ul>	Актуально	

	<p>оператор, объекты, в которых размещены ресурсы информационной системы);</p> <ul style="list-style-type: none"><li>- сведения об информационных технологиях, базах данных, информационных систем, системного программного обеспечения, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, информационные системы и системное программное обеспечение, используемые в информационной системе совместно с СКЗИ;</li><li>- содержание конструкторской документации на СКЗИ;</li><li>- содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;</li><li>- общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;</li><li>- сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);</li><li>- все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;</li><li>- сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;</li><li>- 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;</li><li>- сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ</li></ul>	
--	--	--

<p>подпункт "ж" пункта 10</p>	<p>Применение: - находящихся в свободном доступе или используемых за пределами КЗ информационных систем и системного программного обеспечения, включая аппаратные и программные компоненты СКЗИ и СФ; - специально разработанных информационных систем и программного обеспечения.</p>	<p>Неактуально</p>	<p>Информационные системы и системное программное обеспечение, включая аппаратные и программные компоненты СКЗИ и СФ не находятся в свободном доступе и (или) не используются за пределами КЗ</p>
<p>подпункт "з" пункта 10</p>	<p>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</p>	<p>Неактуально</p>	<p>Используемые каналы связи, защищены от несанкционированного доступа к информации организационными, техническими и (или) криптографическими мерами. Технические каналы утечки информации СКЗИ и линий связи признаны не актуальными (используется оптоволоконные линии связи, витая пара проложена в общих линиях, в которых расположены десятки других витых пар, затраты на использование средств негласного съема информации по техническим каналам утечки информации значительно превышают ценность информации)</p>
<p>подпункт "и" пункта 10</p>	<p>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</p>	<p>Неактуально</p>	<p>Перечень пользователей некоторых информационных систем, имеющих выход в информационно-телекоммуникационную сеть "Интернет", ограничен списком утверждаемым Руководством Операторов информационных систем. Доступ предоставляется по заявке с обоснованием. Не всем пользователям согласуют доступ в информационно-телекоммуникационную сеть "Интернет". Используются технические средства защиты информации от угрозы атаки из информационно-телекоммуникационной сети "Интернет"</p>
<p>подпункт "к" пункта 10</p>	<p>Использование на этапе эксплуатации находящихся за пределами КЗ информационных систем и системного</p>	<p>Неактуально</p>	<p>КЗ программного обеспечения из состава средств</p>

	программного обеспечения из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ	информационной системы, применяемых на местах эксплуатации СКЗИ	
подпункт "а" пункта 11	Проведение атаки, при нахождении в пределах контролируемой зоны	Актуально	
подпункт "б" пункта 11	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится средства вычислительной техники (далее - СВТ), на которых реализованы СКЗИ и СФ.	Актуально	
подпункт "в" пункта 11	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	
подпункт "г" пункта 11	Использование штатных средств информационных систем, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Актуально	
подпункт "а" пункта 12	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Неактуально	- Проводятся работы по подбору персонала; - доступ в КЗ 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.

			<p>оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия только для санкционированного прохода;</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;</li> <li>- осуществляется регистрация и учет действий пользователей;</li> <li>- на АРМ и серверах, на которых установлены СКЗИ, используются сертифицированные средства защиты информации от несанкционированного доступа и сертифицированные средства антивирусной защиты</li> </ul>
<p>подпункт "б" пункта 12</p>	<p>Возможность располагать (воздействовать на) аппаратными(-ые) компонентами(-ы) СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий</p>	<p>Неактуально</p>	<ul style="list-style-type: none"> <li>- Проводятся работы по подбору персонала;</li> <li>- доступ в КЗ и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом;</li> <li>- помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия только для санкционированного прохода;</li> <li>- 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;</li> <li>- осуществляется разграничение и контроль доступа</li> </ul>

			<p>пользователей к защищаемым ресурсам; - осуществляется регистрация и учет действий пользователей</p>
<p>подпункт "а" пункта 13</p>	<p>Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ</p>	<p>Неактуально</p>	<p>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. Доступ в КЗ 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 открытия 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 ответственных сотрудников</p>
<p>подпункт "б" пункта 13</p>	<p>Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченные меры, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий</p>	<p>Неактуально</p>	<p>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. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-</p>



<p>подпункт "а" пункта 13</p>	<p>Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения</p>	<p>Неактуально</p>	<p>пропускным режимом. Помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия 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 ответственных сотрудников</p>
<p>подпункт "в" пункта 13</p>	<p>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 программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ</p>	<p>Неактуально</p>	<p>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. Оператор не является конкурентом производителя прикладного программного обеспечения. Оператором не обрабатываются персональные данные, составляющие коммерческую тайну конкурентов производителя прикладного программного обеспечения. Используется сертифицированные антивирусное программное обеспечение и сканеры уязвимостей</p>

			<p>Оператором не обрабатываются персональные данные, составляющие коммерческую тайну конкурентов производителя прикладного программного обеспечения. Используется сертифицированные антивирусное программное обеспечение и сканеры уязвимостей</p>
<p>подпункт "а" пункта 14</p>	<p>Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного программного обеспечения</p>	<p>Неактуально</p>	<p>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. Используется сертифицированные антивирусное программное обеспечение и сканеры уязвимостей. Средства защиты информации прошли процедуру контроля отсутствия недокументированных возможностей в программном обеспечении</p>
<p>подпункт "б" пункта 14</p>	<p>Возможность располагать сведениями, содержащимися в структурной документации на аппаратные и программные компоненты СФ</p>	<p>Неактуально</p>	<p>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</p>
<p>подпункт "в" пункта 14</p>	<p>Возможность располагать всеми аппаратными компонентами СКЗИ и СФ (воздействовать на любые компоненты СКЗИ и СФ)</p>	<p>Неактуально</p>	<p>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. Доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-</p>

		<p>пропускным режимом.  Помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия 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 ответственных сотрудников</p>
--	--	--

-----

<\*> Состав и содержание 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, утвержденные приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 (Зарегистрирован Минюстом России 18 августа 2014 г., регистрационный N 33620).

Приложение 2  
к приказу инспекции государственного  
жилищного надзора  
Волгоградской области  
от 26 декабря 2022 г. N 260

Перечень угроз безопасности персональных данных, актуальных  
при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности  
инспекции государственного жилищного надзора Волгоградской области, защищаемых  
без использования средств криптографической защиты информации

Идентификатор угрозы безопасности информации <*>	Наименование угрозы безопасности информации	Актуальность использования (применения) для построения и реализации атак	Обоснование неактуальности
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	Неактуальна	Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "средний", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.004	Угроза аппаратного сброса пароля BIOS	Актуальна	
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Неактуальна	Угроза является неактуальной ввиду неактуальности в Инспекции потенциала нарушителя
УБИ.006	Угроза внедрения кода или данных	Актуальна	
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Актуальна	

УБИ.008	Угроза восстановления аутентификационной информации	Актуальна	
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Актуальна	
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Актуальна	
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции технологий беспроводного доступа
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Актуальна	
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Актуальна	
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Актуальна	
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Актуальна	
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Актуальна	
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Актуальна	
УБИ.018	Угроза загрузки нештатной операционной системы	Актуальна	
УБИ.019	Угроза заражения DNS-кеша	Актуальна	
УБИ.020	Угроза злоупотребления возможностями,	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных

	предоставленными потребителям облачных услуг		технологий	
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий	
УБИ.022	Угроза избыточного выделения оперативной памяти	Актуальна		
УБИ.023	Угроза изменения компонентов системы	Актуальна		
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Неактуальна	Для реализации угрозы, внутренний нарушитель должен иметь потенциал не ниже "высокий", актуальный внутренний нарушитель имеет потенциал "средний".	
УБИ.025	Угроза изменения системных и глобальных переменных	Актуальна		
УБИ.026	Угроза искажения XML-схемы	Актуальна		
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Актуальна		
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Актуальна		
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера "паразитными" процессами	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции суперкомпьютеров	
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Актуальна		
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Актуальна		

УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Неактуальна	Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "средний", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.033	Угроза использования слабостей кодирования входных данных	Актуальна	
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Актуальна	
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Неактуальна	Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "высокий", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.036	Угроза исследования механизмов работы программы	Актуальна	
УБИ.037	Угроза исследования приложения через отчеты об ошибках	Актуальна	
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Неактуальна	Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "средний", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.040	Угроза конфликта юрисдикций различных стран	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.041	Угроза межсайтового скрининга	Актуальна	
УБИ.042	Угроза межсайтовой подделки запроса	Актуальна	
УБИ.043	Угроза нарушения доступности облачного сервера	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий

УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Актуальна	
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Актуальна	
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Актуальна	
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.048	Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин	Актуальна	
УБИ.049	Угроза нарушения целостности данных кеша	Актуальна	
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Актуальна	
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Актуальна	
УБИ.053	Угроза невозможности управления	Актуально	



	правами пользователей BIOS			
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий	
УБИ.055	Угроза незащищенного администрирования облачных услуг	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий	
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий	
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных	
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий	
УБИ.059	Угроза неконтролируемого роста числа резервированных вычислительных ресурсов	Актуальна		
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных	
УБИ.061	Угроза некорректного задания структуры данных транзакции	Актуальна		
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера	Актуальна		
УБИ.063	Угроза некорректного использования функционала программного обеспечения	Актуальна		

УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.065	Угроза неопределенности в распределении ответственности между ролями в облаке	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.066	Угроза неопределенности ответственности за обеспечение безопасности облака	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Актуальна	
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Актуальна	
УБИ.069	Угроза неправомерных действий в каналах связи	Актуальна	
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.071	Угроза несанкционированного восстановления удаленной защищаемой информации	Актуальна	
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Актуальна	
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Актуальна	

УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Актуальна	
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Актуальна	
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Актуальна	
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Актуальна	
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Актуальна	
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Актуальна	
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Актуальна	
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции суперкомпьютеров
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции технологий беспроводного доступа

УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Актуальна	
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Актуальна	
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Актуальна	
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Актуальна	
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Актуальна	
УБИ.089	Угроза несанкционированного редактирования реестра	Актуальна	
УБИ.090	Угроза несанкционированного создания учетной записи пользователя	Актуальна	
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Актуальна	
УБИ.092	Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам	Неактуальна	Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "высокий", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.093	Угроза несанкционированного управления буфером	Актуальна	
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Актуальна	

УБИ.095	Угроза несанкционированного управления указателями	Актуальна	
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.097	Угроза несогласованности правил доступа к большим данным	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Актуальна	
УБИ.099	Угроза обнаружения хостов	Актуальна	
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Актуальна	
УБИ.101	Угроза общедоступности облачной инфраструктуры	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Актуальна	
УБИ.103	Угроза определения типов объектов защиты	Актуальна	
УБИ.104	Угроза определения топологии вычислительной сети	Актуальна	
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.106	Угроза отказа в обслуживании системой	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции

	хранения данных суперкомпьютера		суперкомпьютеров
УБИ.107	Угроза отключения контрольных датчиков	Актуальна	
УБИ.108	Угроза ошибки обновления гипервизора	Актуальна	
УБИ.109	Угроза перебора всех настроек и параметров приложения	Актуальна	
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.111	Угроза передачи данных по скрытым каналам	Актуальна	
УБИ.112	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции оборудования с числовым программным управлением
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Актуальна	
УБИ.114	Угроза переполнения целочисленных переменных	Актуальна	
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Актуальна	
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Актуальна	
УБИ.117	Угроза перехвата привилегированного потока	Актуальна	
УБИ.118	Угроза перехвата привилегированного процесса	Актуальна	

УБИ.119	Угроза перехвата управления гипервизором	Актуальна	
УБИ.120	Угроза перехвата управления средой виртуализации	Актуальна	
УБИ.121	Угроза повреждения системного реестра	Актуальна	
УБИ.122	Угроза повышения привилегий	Актуальна	
УБИ.123	Угроза подбора пароля BIOS	Актуальна	
УБИ.124	Угроза подделки записей журнала регистрации событий	Актуальна	
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции технологий беспроводного доступа
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции технологий беспроводного доступа
УБИ.127	Угроза подмены действия пользователя путем обмана	Актуальна	
УБИ.128	Угроза подмены доверенного пользователя	Актуальна	
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Актуальна	
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Актуальна	
УБИ.131	Угроза подмены субъекта сетевого доступа	Актуальна	
УБИ.132	Угроза получения предварительной информации об объекте защиты	Актуальна	

УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции технологий беспроводного доступа
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.137	Угроза потери управления облачными ресурсами	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе ее в облако	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.139	Угроза преодоления физической защиты	Актуальна	
УБИ.140	Угроза приведения системы в состояние "отказ в обслуживании"	Актуальна	
УБИ.141	Угроза привязки к поставщику облачных услуг	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Актуальна	
УБИ.144	Угроза программного сброса пароля BIOS	Актуальна	



УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Актуальна	
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции суперкомпьютеров
УБИ.147	Угроза распространения несанкционированного повышенных прав на всю грид-систему	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции грид-систем
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции хранилищ больших данных
УБИ.149	Угроза сбоя обработки специальным образом измененных файлов	Актуальна	
УБИ.150	Угроза сбоя процесса обновления BIOS	Актуальна	
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Актуальна	
УБИ.152	Угроза удаления аутентификационной информации	Актуальна	
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Актуальна	
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Актуальна	
УБИ.155	Угроза утраты вычислительных ресурсов	Актуальна	
УБИ.156	Угроза утраты носителей информации	Актуальна	

УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Актуальна	
УБИ.158	Угроза форматирования носителей информации	Актуальна	
УБИ.159	Угроза "форсированного веб-браузинга"	Неактуальна	Отсутствуют объекты воздействия угрозы
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Актуальна	
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции суперкомпьютеров
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Актуальна	
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Актуальна	
УБИ.164	Угроза распространения состояния "отказ в обслуживании" в облачной инфраструктуре	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции облачных технологий
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Актуальна	
УБИ.166	Угроза внедрения системной избыточности	Актуальна	
УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов	Актуальна	

УБИ.168	Угроза "кражи" учетной записи доступа к сетевым сервисам	Актуальна	
УБИ.169	Угроза наличия механизмов разработчика	Актуальна	
УБИ.170	Угроза неправомерного шифрования информации	Актуальна	
УБИ.171	Угроза скрытого включения вычислительного устройства в состав бот-сети	Актуальна	
УБИ.172	Угроза распространения "почтовых червей"	Актуальна	
УБИ.173	Угроза "спама" веб-сервера	Актуальна	
УБИ.174	Угроза "фарминга"	Актуальна	
УБИ.175	Угроза "фишинга"	Актуальна	
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Актуальна	
УБИ.177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Актуальна	
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Актуальна	
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Актуальна	

УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Актуальна	
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Актуальна	
УБИ.182	Угроза физического устаревания аппаратных компонентов	Актуальна	
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции автоматизированных систем управления технологическими процессами
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Неактуальна	Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Актуальна	
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Актуальна	
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Актуальна	
УБИ.188	Угроза подмены программного обеспечения	Актуальна	
УБИ.189	Угроза маскирования действий вредоносного кода	Актуальна	
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в информационно-телекоммуникационной	Актуальна	

	сети "Интернет"			
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Актуальна		
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Актуальна		
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика	Актуальна		
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Неактуальна		Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Неактуальна		Для реализации угрозы, внешний нарушитель должен иметь потенциал ниже "высокий", актуальный нарушитель имеет потенциал "низкий"
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Неактуальна		Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Актуальна		
УБИ.198	Угроза скрытой регистрации вредоносной программой учетных записей администраторов	Актуальна		
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Неактуальна		Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств

УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Неактуальна	Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Актуальна	
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Неактуальна	Угроза является неактуальной ввиду отсутствия в системах Инспекции возможности обработки данных при помощи мобильных устройств
УБИ.203	Угроза утечки информации с неподключенных к информационно-телекоммуникационной сети "Интернет" компьютеров	Актуальна	
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции автоматизированных систем управления технологическими процессами
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Актуальна	
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции оборудования с числовым программным управлением
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования "мастер-кодов"	Неактуальна	Угроза является неактуальной ввиду отсутствия в Инспекции оборудования с числовым программным управлением

	(инженерных паролей)			
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Актуальна		
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Актуальна		
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Неактуальна		Для реализации угрозы, внутренний нарушитель должен иметь потенциал не ниже "высокий", актуальный внутренний нарушитель имеет потенциал "средний".
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Актуальна		
УБИ.212	Угроза перехвата управления информационной системой	Актуальна		
УБИ.213	Угроза обхода многофакторной аутентификации	Неактуальна		Для реализации угрозы, внешний нарушитель должен иметь потенциал не ниже "высокий", актуальный внешний нарушитель имеет потенциал "низкий"
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Актуальна		
УБИ.215	Угроза несанкционированного доступа к	Актуальна		

	системе при помощи сторонних сервисов			
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе Smart-карт	
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Актуальна		
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе технологий искусственного интеллекта	
УБИ.219	Угроза хищения обучающих данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе технологий искусственного интеллекта	
УБИ.220	Угроза нарушения функционирования ("обхода") средств, реализующих технологии искусственного интеллекта	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе технологий искусственного интеллекта	
УБИ.221	Угроза модификации модели машинного обучения путем искажения ("отравления") обучающих данных	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе технологий искусственного интеллекта	
УБИ.222	Угроза подмены модели машинного обучения	Неактуальна	Угроза является неактуальной ввиду отсутствия в Системе технологий искусственного интеллекта	

-----  
 <\*> Согласно банку данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).