Приложение

к распоряжению Правительства Тверской области

от 24.08.2018 № 380-рп

Угрозы безопасности персональных данных,

 актуальные при обработке персональных данных

в информационных системах персональных данных

исполнительных органов государственной власти Тверской области

и государственных учреждений Тверской области

Раздел I

Общие положения

1. Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных в исполнительных органах государственной власти Тверской области и в государственных учреждениях Тверской области (далее – Актуальные угрозы безопасности ИСПДн), разработаны в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», 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 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», 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».

2. Персональные данные субъектов персональных данных в исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области обрабатываются с целью получения государственных услуг, а также:

1) в целях обеспечения деятельности Губернатора Тверской области и Правительства Тверской области;

2) в целях обеспечения кадровой работы в исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области, в целях содействия государственным гражданским служащим Тверской области при исполнении ими своих должностных обязанностей, в обучении и должностном росте, обеспечения установленных законодательством Российской Федерации условий осуществления служебной деятельности и труда, гарантий и компенсаций, обеспечения личной безопасности государственных гражданских служащих Тверской области, работников и членов их семей, обеспечения сохранности принадлежащего им имущества и государственного имущества Тверской области;

3) в целях ведения бухгалтерского учета в исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области;

4) в целях реализации полномочий исполнительных органов государственной власти Тверской области;

5) в целях реализации задач и функций государственных учреждений Тверской области;

6) в целях формирования кадрового резерва на государственной гражданской службе Тверской области, резерва управленческих кадров Тверской области, противодействия коррупции;

7) в целях реализации процедур по представлению граждан к награждению;

8) в целях приема, обработки и распределения поступивших в адрес Губернатора Тверской области, Правительства Тверской области, областных исполнительных органов государственной власти Тверской области документов, обращений граждан и организаций, а также регистрации и отправки исходящей корреспонденции;

9) в целях ведения внутренней служебной переписки;

10) в целях формирования внутренних документов, регламентирующих деятельность исполнительных органов государственной власти Тверской области;

11) в целях выдачи пропусков для прохода в здания Правительства Тверской области;

12) в целях подготовки и проведения мероприятий с участием или по поручению Губернатора Тверской области, подготовки пресс-релизов о деятельности Правительства Тверской области, взаимодействия со сторонними средствами массовой информации.

3. Контролируемой зоной информационной системы персональных данных (далее – контролируемая зона) являются здания и помещения исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области, в которых исключено неконтролируемое пребывание сотрудников исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области и посетителей. В пределах контролируемой зоны находятся рабочие места пользователей, серверы системы, сетевое и телекоммуникационное оборудование информационной системы персональных данных (далее – ИСПДн). Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

4. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн.

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных.

5. Угрозы безопасности персональных данных, актуальные при обработке персональных данных, уточняются и дополняются по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн. Указанные изменения согласовываются с ФСТЭК России и ФСБ России в установленном порядке.

6. Актуальные угрозы безопасности ИСПДн подлежат адаптации в ходе разработки исполнительными органами государственной власти Тверской области, государственными учреждениями Тверской области частных моделей угроз безопасности персональных данных для каждой ИСПДн.

7. В частной модели угроз безопасности персональных данных указываются:

1) описание ИСПДн и ее структурно-функциональных характеристик;

2) описание угроз безопасности персональных данных с учетом совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

3) описание возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Раздел II

Общее описание информационных систем персональных данных,

эксплуатируемых в исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области

8. В исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области эксплуатируется два типа ИСПДн: локальные и распределенные.

Локальные ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области имеют сходную структуру, одноточечное подключение к сетям общего пользования и (или) сетям международного информационного обмена, обрабатывают различные категории персональных данных и имеют уровень защищенности до третьего включительно.

Распределенные ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области имеют сходную структуру, имеют многоточечное подключение к сетям общего пользования и (или) сетям международного информационного обмена, обрабатывают различные категории персональных данных и имеют уровень защищенности до первого включительно.

Передача персональных данных в распределенных ИСПДн осуществляется по информационно-телекоммуникационным сетям общего пользования, в которых возможен несанкционированный доступ к передаваемой по ним защищаемой информации. Для обеспечения защиты информации при передаче персональных данных в распределенных ИСПДн используются сертифицированные средства криптографической защиты информации (далее – СКЗИ).

9. Для ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области актуальны угрозы безопасности персональных данных второго и третьего типа, не связанные с наличием недекларированных возможностей в системном программном обеспечении, используемом в ИСПДн.

10. Основными характеристиками безопасности, которые необходимо обеспечивать для обрабатываемых персональных данных являются:

1) 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;

2) целостность – состояние защищенности информации, характеризуемое способностью ИСПДн обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения;

3) доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

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

12. Рабочие места пользователей, серверы, сетевое и телекоммуникационное оборудование ИСПДн находятся в пределах контролируемых зон. Вне контролируемых зон находятся каналы передачи данных.

13. В административных зданиях исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области организован пропускной режим, неконтролируемое пребывание посторонних лиц и неконтролируемое перемещение (вынос за пределы здания) компьютеров и оргтехники исключено. Помещения оборудованы запирающимися дверями. Административные здания исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области могут быть оборудованы системами видеонаблюдения.

14. Защита персональных данных в ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области обеспечивается средствами защиты информации (далее – СЗИ):

1) СЗИ от несанкционированного доступа;

2) средствами антивирусной защиты;

3) межсетевыми экранами;

4) СКЗИ.

Раздел III

 Определение актуальности использования СКЗИ

для обеспечения безопасности персональных данных

15. Актуальность применения СКЗИ в ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области определяется необходимостью защиты персональных данных при их передаче по сетям общего пользования и (или) сетям международного информационного обмена.

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

17. Принятыми организационно-техническими мерами в исполнительных органах государственной власти Тверской области и государственных учреждениях Тверской области исключена возможность несанкционированного доступа к ключевой информации СКЗИ.

18. Объектами защиты в ИСПДн с использованием СКЗИ являются:

1. персональные данные;
2. СКЗИ;
3. среда функционирования СКЗИ (далее – СФ);
4. информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
5. 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 СФ;
6. носители защищаемой информации, используемые в ИСПДн, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
7. используемые ИСПДн каналы (линии) связи, включая кабельные системы;
8. помещения, в которых находятся ресурсы ИСПДн, имеющие отношение к криптографической защите персональных данных.

Раздел IV

 Определение перечня актуальных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных исполнительных органов

государственной власти Тверской области

и государственных учреждений Тверской области

1. В качестве потенциальных источников атак рассматриваются лица, имеющие доступ к ИСПДн. К таким лицам относятся сотрудники исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области, в том числе администраторы ИСПДн, посетители исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области, а также внешние нарушители.
2. Сотрудники исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области, в том числе администраторы ИСПДн, имеют постоянный доступ в контролируемую зону и доступ к объектам защиты. При поступлении граждан на гражданскую службу или на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области, они должны быть ознакомлены сотрудниками кадровых подразделений данных исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области с правилами работы в ИСПДн и мерами ответственности за несоблюдение правил обеспечения безопасности информации.
3. Посетители исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области имеют разовый доступ в контролируемую зону. Посетители исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области могут находиться в контролируемой зоне в непосредственной близости к объектам защиты только в присутствии сотрудников исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области.

22. Внешние нарушители способны осуществлять попытки несанкционированного доступа к информации в ИСПДн из-за границы контролируемой зоны, в том числе с использованием сетей общего пользования и (или) сетей международного информационного обмена.

23. На основании исходных данных об объектах защиты и источниках атак в приложении 1 определены обобщенные возможности источников атак для ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области.

24. В соответствии с обобщенными возможностями источников атак для ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области в приложении 2 определены уточненные возможности нарушителей и направления атак.

25. В настоящее время в ИСПДн не применяются технологии, связанные с использованием грид-систем (систем, использующих технологии распределенных вычислений), хранилищ больших данных, трансграничной передачей защищаемой информации. Из перечня актуальных угроз безопасности персональных данных могут быть исключены угрозы, связанные с использованием данных технологий.

26. На основе анализа рекомендуемого ФСТЭК России банка данных угроз безопасности информации с учетом структурно-функциональных характеристик ИСПДн, а также применяемых в них информационных технологий и особенностей функционирования, в ИСПДн исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области могут быть актуальны угрозы безопасности, указанные в приложении 3.

27. Угрозы безопасности персональных данных, обрабатываемых в ИСПДн, указанные в приложении 3, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн.

Приложение 1

к Угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области

|  |  |  |
| --- | --- | --- |
| № п/п | Обобщенные возможности источников атак | Да/Нет |
|  | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны | Да |
|  | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы средства криптографической защиты информации (далее – СКЗИ) и среда их функционирования | Да |
|  | Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования | Нет |
|  | 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 |
|  | Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения) | Нет |
|  | 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 |

Приложение 2

к Угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области

Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)

| №п/п | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) для построения и реализации атак | Обоснование отсутствия |
| --- | --- | --- | --- |
|  | Проведение атаки при нахождении в пределах контролируемой зоны | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области;посетители исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области могут находиться в контролируемой зоне в непосредственной близости к объектам защиты только в присутствии сотрудников исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области;сотрудники, являющиеся пользователями информационных систем персональных данных (далее – ИСПДн), но не являющиеся пользователями средств криптографической защиты информации (далее – СКЗИ), проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;пользователи СКЗИ проинформированыо правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации;помещения, в которых располагаются СКЗИ, оборудованы входными дверями с замками, обеспечивающими постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях;утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ;осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;осуществляется регистрация и учет действий пользователей с персональными данными;осуществляется контроль целостности средств защиты;на автоматизированных рабочих местах и серверах, на которых установлены СКЗИ, используются сертифицированные средства защиты информации от несанкционированного доступа;используются сертифицированные средства антивирусной защиты |
|  | Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:документацию на СКЗИ и компоненты среды функционирования;помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе средств вычислительной техники и компоненты среды функционирования | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе;помещения, в которых располагается документация на СКЗИ, СКЗИ и компоненты среды функционирования, оборудованы входными дверями с замками, обеспечивающими постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода;утвержден перечень лиц, имеющих право доступа в помещения |
|  | 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 средства вычислительной техники, на которых реализованы СКЗИ и компоненты среды функционирования | Актуально |   |
|  | Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий | Актуально |   |
|  | Физический доступ к средствам вычислительной техники, на которых реализованы СКЗИ и компоненты среды функционирования | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области;помещения, в которых располагаются средства вычислительной техники, на которых располагаются СКЗИ и компоненты среды функционирования, оборудованы входными дверями с замками, обеспечивающими постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода |
|  | Возможность воздействовать на аппаратные компоненты СКЗИ и компоненты среды функционирования, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ,и направленными на предотвращение и пресечение несанкционированных действий | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области;помещения, в которых располагаются СКЗИ и компоненты среды функционирования, оснащены входными дверями 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 компоненты среды функционирования, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников исполнительных органов государственной власти Тверской областии государственных учреждений Тверской области |
|  | Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, функционирование СКЗИ и компоненты среды функционирования в области использования для реализации недекларированных возможностей прикладного программного обеспечения | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области;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;помещения, в которых располагаются СКЗИ и компоненты среды функционирования, оборудованы входными дверями с замками, обеспечивающими 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 компоненты среды функционирования, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области;осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;осуществляется регистрация и учет действий пользователей;на автоматизированных рабочих местах и серверах, на которых установлены СКЗИ: используются сертифицированные СЗИ от несанкционированного доступа к информации;используются сертифицированные средства антивирусной защиты |
|  | 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 нарушителей |
|  | Проведение работ по созданию способов и средств атакв научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и компонентов среды функционирования, в том числе с использованием исходных текстов входящего в среду функционирования прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интересдля реализации возможности;высокая стоимость и сложность подготовки реализации возможности нарушителей |
|  | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недекларированных возможностей системного программного обеспечения | Неактуально | Осуществляется отбор кандидатов на гражданскую службу и на работу в исполнительные органы государственной власти Тверской области и государственные учреждения Тверской области;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;помещения, в которых располагаются СКЗИ и компоненты среды функционирования, оборудованы входными дверями с замками, обеспечивающими 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 компоненты среды функционирования, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области;осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам;осуществляется регистрация и учет действий пользователей;на автоматизированных рабочих местах и серверах, на которых установлены СКЗИ используются сертифицированные средства защиты информации от несанкционированного доступа к информации;используются сертифицированные средства антивирусной защиты |
|  | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности |
|  | Возможность воздействовать на любые компоненты СКЗИ и среды функционирования | Неактуально | Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности |

Приложение 3

к Угрозам безопасности персональных данных, актуальным при обработке персональных данных в информационных системах персональных данных исполнительных органов государственной власти Тверской области и государственных учреждений Тверской области

Угрозы безопасности персональных данных,

актуальные при обработке персональных данных

в информационных системах персональных данных

исполнительных органов государственной власти Тверской области

и государственных учреждений Тверской области

1. Угроза анализа криптографических алгоритмов и их реализации.
2. Угроза аппаратного сброса пароля BIOS.
3. Угроза внедрения вредоносного кода в BIOS.
4. Угроза внедрения кода или данных.
5. Угроза воздействия на программы с высокими привилегиями.
6. Угроза восстановления аутентификационной информации.
7. Угроза восстановления предыдущей уязвимой версии BIOS.
8. Угроза выхода процесса за пределы виртуальной машины.
9. Угроза деструктивного изменения конфигурации/среды окружения программ.
10. Угроза доступа к защищаемым файлам с использованием обходного пути.
11. Угроза доступа к локальным файлам сервера при помощи URL.
12. Угроза доступа/перехвата/изменения HTTP cookies.
13. Угроза загрузки нештатной операционной системы.
14. Угроза заражения DNS-кеша.
15. Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг.
16. Угроза избыточного выделения оперативной памяти.
17. Угроза изменения компонентов системы.
18. Угроза изменения системных и глобальных переменных.
19. Угроза искажения XML-схемы.
20. Угроза искажения вводимой и выводимой на периферийные устройства информации.
21. Угроза использования альтернативных путей доступа к ресурсам.
22. Угроза использования механизмов авторизации для повышения привилегий.
23. Угроза использования поддельных цифровых подписей BIOS.
24. Угроза использования слабостей кодирования входных данных.
25. Угроза использования слабостей протоколов сетевого/локального обмена данными.
26. Угроза исследования приложения через отчеты об ошибках.
27. Угроза исчерпания запаса ключей, необходимых для обновления BIOS.
28. Угроза межсайтового скриптинга.
29. Угроза межсайтовой подделки запроса.
30. Угроза нарушения доступности облачного сервера.
31. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины.
32. Угроза нарушения технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин.
33. Угроза нарушения целостности данных кеша.
34. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания.
35. Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения.
36. Угроза невозможности управления правами пользователей BIOS.
37. Угроза недобросовестного исполнения обязательств поставщиками облачных услуг.
38. Угроза незащищенного администрирования облачных услуг.
39. Угроза некачественного переноса инфраструктуры в облако.
40. Угроза неконтролируемого роста числа виртуальных машин.
41. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов.
42. Угроза некорректного задания структуры данных транзакции.
43. Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера.
44. Угроза некорректного использования функционала программного обеспечения.
45. Угроза некорректной реализации политики лицензирования в облаке.
46. Угроза неопределенности в распределении ответственности между ролями в облаке.
47. Угроза неопределенности ответственности за обеспечение безопасности облака.
48. Угроза неправомерного ознакомления с защищаемой информацией.
49. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.
50. Угроза неправомерных действий в каналах связи.
51. Угроза непрерывной модернизации облачной инфраструктуры.
52. Угроза несанкционированного восстановления удаленной защищаемой информации.
53. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS.
54. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.
55. Угроза несанкционированного доступа к аутентификационной информации.
56. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети.
57. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети.
58. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение.
59. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети.
60. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин.
61. Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети.
62. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации.
63. Угроза несанкционированного изменения аутентификационной информации.
64. Угроза несанкционированного использования привилегированных функций BIOS.
65. Угроза несанкционированного копирования защищаемой информации.
66. Угроза несанкционированного редактирования реестра.
67. Угроза несанкционированного создания учетной записи пользователя.
68. Угроза несанкционированного удаления защищаемой информации.
69. Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам.
70. Угроза несанкционированного управления буфером.
71. Угроза несанкционированного управления синхронизацией и состоянием.
72. Угроза несанкционированного управления указателями.
73. Угроза несогласованности политик безопасности элементов облачной инфраструктуры.
74. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб.
75. Угроза обнаружения хостов.
76. Угроза обхода некорректно настроенных механизмов аутентификации.
77. Угроза общедоступности облачной инфраструктуры.
78. Угроза опосредованного управления группой программ через совместно используемые данные.
79. Угроза определения типов объектов защиты.
80. Угроза определения топологии вычислительной сети.
81. Угроза ошибки обновления гипервизора.
82. Угроза перебора всех настроек и параметров приложения.
83. Угроза передачи данных по скрытым каналам.
84. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники.
85. Угроза переполнения целочисленных переменных.
86. Угроза перехвата вводимой и выводимой на периферийные устройства информации.
87. Угроза перехвата данных, передаваемых по вычислительной сети.
88. Угроза перехвата привилегированного потока.
89. Угроза перехвата привилегированного процесса.
90. Угроза перехвата управления гипервизором.
91. Угроза перехвата управления средой виртуализации.
92. Угроза повреждения системного реестра.
93. Угроза повышения привилегий.
94. Угроза подбора пароля BIOS.
95. Угроза подделки записей журнала регистрации событий.
96. Угроза подмены действия пользователя путем обмана.
97. Угроза подмены доверенного пользователя.
98. Угроза подмены резервной копии программного обеспечения BIOS.
99. Угроза подмены содержимого сетевых ресурсов.
100. Угроза потери доверия к поставщику облачных услуг.
101. Угроза потери и утечки данных, обрабатываемых в облаке.
102. Угроза потери управления облачными ресурсами.
103. Угроза потери управления собственной инфраструктурой при переносе ее в облако.
104. Угроза подмены субъекта сетевого доступа.
105. Угроза получения предварительной информации об объекте защиты.
106. Угроза получения сведений о владельце беспроводного устройства.
107. Угроза преодоления физической защиты.
108. Угроза приведения системы в состояние «отказ в обслуживании».
109. Угроза привязки к поставщику облачных услуг.
110. Угроза приостановки оказания облачных услуг вследствие технических сбоев.
111. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
112. Угроза программного сброса пароля BIOS.
113. Угроза пропуска проверки целостности программного обеспечения.
114. Угроза, сбоя обработки специальным образом измененных файлов.
115. Угроза сбоя процесса обновления BIOS.
116. Угроза удаления аутентификационной информации.
117. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов.
118. Угроза установки уязвимых версий обновления программного обеспечения BIOS.
119. Угроза утраты вычислительных ресурсов.
120. Угроза утраты носителей информации.
121. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации.
122. Угроза форматирования носителей информации.
123. Угроза «форсированного веб-браузинга».
124. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации.
125. Угроза эксплуатации цифровой подписи программного кода.
126. Угроза перехвата исключения/сигнала из привилегированного блока функций.
127. Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре.
128. Угроза включения в проект не достоверно испытанных компонентов.
129. Угроза внедрения системной избыточности.
130. Угроза заражения компьютера при посещении неблагонадежных сайтов.
131. Угроза «кражи» учетной записи доступа к сетевым сервисам.
132. Угроза наличия механизмов разработчика.
133. Угроза неправомерного шифрования информации.
134. Угроза скрытного включения вычислительного устройства в состав бот-сети.
135. Угроза распространения «почтовых червей».
136. Угроза «спама» веб-сервера.
137. Угроза «фарминга».
138. Угроза «фишинга».
139. Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты.
140. Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью.
141. Угроза несанкционированного использования системных и сетевых утилит.
142. Угроза несанкционированной модификации защищаемой информации.
143. Угроза отказа подсистемы обеспечения температурного режима.
144. Угроза перехвата одноразовых паролей в режиме реального времени.
145. Угроза физического устаревания аппаратных компонентов.
146. Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства.
147. Угроза несанкционированного изменения параметров настройки средств защиты информации.
148. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.
149. Угроза несанкционированного воздействия на средство защиты информации.
150. Угроза подмены программного обеспечения.
151. Угроза маскирования действий вредоносного кода.
152. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет.
153. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.
154. Угроза использования уязвимых версий программного обеспечения.
155. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика.