УТВЕРЖДАЮ:
«__» _____ 20__ г.

СТО № ИБ.001

Методика моделирования угроз информационной безопасности ООО «Сатурн»

Версия 1.0

Москва
2018

Сведения о нормативном документе

Информация о документе	
Функциональный руководитель	
Разработчик документа	
Введен в действие	Приказом № _____ от ___.___._____
Срок действия	не ограничен

История изменений			
Дата	**Версия**	**Автор изменений**	**Причина внесения изменений**

Содержание

1. Цель и область действия

1.1 Цель Методики

Целью разработки методики моделирования угроз информационной безопасности ООО «Сатурн» (далее – Методика) является повышение уровня информационной безопасности ООО «Сатурн», а также обеспечение демонстрации того, что Корпорация своевременно и адекватно реагирует на угрозы информационной безопасности.

1.2 Область действия

1.2.1 Настоящая Методика:

1.2.1.1 Определяет системный и методический подход к определению угроз информационной безопасности и разработке моделей угроз информационной безопасности.

1.2.1.2 Описывает перечень возможных угроз информационной безопасности.

1.2.1.3 Определяет методику разработки моделей угроз для различных Активов и способы оценки актуальных угроз информационной безопасности.

1.2.1.4 Предназначена для применения в работе Дирекции по информационной безопасности ООО «Сатурн», а также при заказе и приемке соответствующих работ по разработке моделей угроз информационной безопасности со стороны подрядных организаций.

1.2.1.5 Распространяется на Активы ООО «Сатурн», находящиеся в зоне ответственности Комплекса по стратегии ООО «Сатурн».

1.2.1.6 Обеспечивает формальное соответствие требованиям законодательства Российской Федерации и нормативно-правовых актов в области информационной безопасности, устанавливаемых к разрабатываемым моделям угроз ИБ.

1.3 Ответственный за актуализацию

Ответственным за актуализацию настоящей Методики является Директор по эксплуатации систем информационной безопасности ООО «Сатурн».

1.4 Общие сведения

Методика разработана на основе проекта Методики определения угроз информационной безопасности в информационных системах, опубликованной ФСТЭК России в 2015 г. на официальном сайте по адресу: https://fstec.ru/component/attachments/download/812.

2. Нормативные ссылки

2.1 ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

2.2 ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Менеджмент риска информационной безопасности.

2.3 СТО № ИБ.002. Регламент управления уязвимостями информационной безопасности ООО «Сатурн».

2.4 СТО № ИБ.003. Регламент управления рисками информационной безопасности ООО «Сатурн».

3. Термины и сокращения

3.1 В настоящей Методике использованы следующие сокращения:

3.1.1 БДУ ФСТЭК – Банк данных угроз ФСТЭК России

3.1.2 ИБ – Информационная безопасность

3.1.3 ДИБ – Дирекция по информационной безопасности ООО «Сатурн»

3.1.4 КпС – Комплекс по стратегии ООО «Сатурн»

3.1.5 ФСТЭК России – Федеральная служба по техническому и экспортному контролю России

3.2 В настоящей Методике использованы следующие термины:

3.2.1 Активы – информация, данные, программное обеспечение и программно-технические средства (включая их окружение) как отдельно, так и в составе автоматизированных и информационных систем, в том числе находящиеся в эксплуатации и планируемые к внедрению/разработке, находящиеся в зоне ответственности Комплекса по стратегии ООО «Сатурн». Следует учитывать, что владельцами данных и информации в большинстве случаев являются структурные подразделения Корпорации, а КпС обеспечивает сервисы хранения, обработки и передачи указанных данных и информации.

3.2.2 Атака - попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования.

3.2.3 Источник угрозы – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

3.2.4 Нарушитель – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах (Активах).

Примечания.

Различают внешнего и внутреннего нарушителей. Под внутренним нарушителем понимают нарушителя, находящегося внутри информационной системы (Актива) на момент начала реализации угрозы. Под внешним нарушителем понимают нарушителя, находящегося вне информационной системы (Актива) на момент начала реализации угрозы.

Для реализации угроз в информационной системе (Актива) внешний нарушитель должен тем или иным способом получить доступ к процессам, проходящим в информационной системе. При этом дальнейшие свои действия внешний нарушитель выполняет от имени, созданного им нового или существующего в системе субъекта.

К внутренним нарушителям относят инсайдеров, несмотря на то, что они могут выполнять инструкции лиц, находящихся вне информационной системы (Актива)

3.2.5 Риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

3.2.6 Угроза ИБ (угроза информационной безопасности) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения информационной безопасности.

3.2.7 Уязвимость - недостаток (слабость) Актива, который (которая) может быть использована для реализации угроз ИБ (информационной безопасности).

4. Общие положения

4.1 Методика применяется на этапах создания Активов для определения и оценки угроз ИБ и разработки моделей угроз, а также в ходе эксплуатации Активов при периодическом пересмотре (переоценке) угроз ИБ.

4.2 Методика применяется совместно с БДУ ФСТЭК (bdu.fstec.ru) в соответствии с Приложением № 1 к Методике, а также базовыми и типовыми моделями угроз ИБ в информационных системах различных классов и типов, разрабатываемых ФСТЭК России.

4.3 Дополнительно при разработке моделей и определения угроз ИБ ДИБ применяет другие каталоги угроз в частности:

– Каталоги угроз ИБ других организаций;

– Собственный каталог угроз ИБ.

4.4 В случае если Актив относится к информационным системам персональных данных, то в соответствии с пунктом 1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», разработанная на основе настоящей Методики модель угроз информационной безопасности должна быть дополнена до соответствия с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России».

4.5 Разработку моделей угроз для Активов осуществляет ДИБ или специализированная подрядная организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации по заказу ДИБ, как отдельно, так и в составе работ по созданию или модернизации Активов.

4.6 В основном модель угроз ИБ разрабатывается для Активов класса информационная/автоматизированная система. Разработка моделей угроз для более простых Активов (как информационный ресурс, или сервер) происходит в упрощенной форме и необходима в редких случаях, поскольку являются обычно частным случаем модели угроз для информационной или автоматизированной системы. *Далее по тексту Методики с позиций ИБ применяется термин информационная система. По тексту методики под термином Актив преимущественно понимается информационная система.*

4.7 Для разработки модели угроз ИБ обязательными условиями является наличие следующих исходных данных:

– Проектная документация на Активы;

– Рабочая документация на Активы

– Эксплуатационная документация на Активы;

– Схема комплекса технических средств;

– Схема информационного взаимодействия компонентов Актива;

– Схема, сетевая отражающая взаимодействия Актива и его компонентов на физическом и логическом уровнях.

– Перечень уязвимостей Активов.

4.8 Итоговая модель угроз информационной безопасности, сформированная на основании указанной методики, составляет сведения, содержащую коммерческую тайну ООО «Сатурн».

4.9 Дирекция по информационной безопасности является центром компетенции (и по указанным далее положениям не предоставляет дополнительных разъяснений или подтверждений):

– по определению потенциала и наличия ресурсов у злоумышленника;

– по определению возможности эксплуатации уязвимостей информационной безопасности.

4.10 Методика ориентирована на определение и оценку антропогенных угроз ИБ, возникновение которых обусловлено объективными факторами. Вместе с тем, часть приведенных в Методике подходов может также применяться для оценки техногенных угроз в случае, если они позволяют достичь целей такой оценки. Определение угроз, связанных со стихийными бедствиями и природными явлениями осуществляется в соответствии с правилами, установленными уполномоченными федеральными органами исполнительной власти, национальными стандартами и находятся за рамками настоящей Методики.

4.11 Действующие модели угроз ИБ, должны пересматриваться минимум в следующих случаях:

– Изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации (в случае обязательности их соблюдения);

– Изменения конфигурации (состава основных компонентов) и особенностей функционирования Активов, следствием которых стало возникновение новых угроз ИБ;

– Выявления уязвимостей, приводящих к возникновению новых угроз ИБ или к повышению возможности реализации существующих;

– Появления сведений и фактов о новых возможностях нарушителей.

4.12 В случае, если в соответствии с настоящей Методикой к числу актуальных угроз, отнесены угрозы, связанные с утечкой информации по техническим каналам, дальнейшая их оценка проводится в соответствии со специальными требованиями и рекомендациями по технической защите конфиденциальной информации и методиками оценки защищенности конфиденциальной информации.

5. Процесс определения угроз ИБ

5.1 Целью определения угроз ИБ является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в Активе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных.

5.2 Определение угроз ИБ должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы. Систематический подход к определению угроз ИБ необходим для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную систему защиты информации в Активе. Меры защиты информации, принимаемые обладателем информации и оператором, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз ИБ, в результате реализации которых возможно наступление неприемлемых негативных последствий (ущерба).

5.3 Систематический подход к определению угроз ИБ предусматривает реализацию непрерывного процесса, в рамках которого определяется область применения процесса определения угроз, идентифицируются источники угроз и угрозы ИБ, оценивается возможность реализации угроз ИБ и степень возможного ущерба в случае такой реализации, осуществляется мониторинг (периодический пересмотр) и переоценка угроз ИБ.

5.4 Оценка угроз ИБ проводится экспертным методом.

5.5 Любое решение, принимаемое экспертами при определении угроз ИБ, должно исходить из правил, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности (принципа «гарантированности»).

5.6 При проведении экспертной оценки принимаются меры, направленные на снижение уровня субъективности и неопределенности при определении каждой из угроз ИБ.

5.7 Экспертную оценку рекомендуется проводить в отношении, как минимум, следующих параметров:

– цели реализации угроз ИБ (мотивация нарушителей);

– типы и виды нарушителей;

– уязвимости, которые могут быть использованы для реализации угроз ИБ;

– способы реализации угроз ИБ;

– степень воздействия угрозы ИБ на каждое из свойств безопасности информации;

– последствия от реализации угроз ИБ; вероятность реализации угроз ИБ; уровень защищенности информационной системы;

– потенциал нарушителя, требуемый для реализации угрозы ИБ (в случае отсутствия потенциала в банке данных угроз ИБ).

5.8 Область применения процесса определения угроз ИБ

5.8.1 На этапах принятия решения о необходимости защиты информации в Активе и разработки требований к защите информации должны быть определены физические и логические границы информационной системы, в которых принимаются и контролируются меры защиты информации, за которые ответственен оператор, а также определены объекты защиты и сегменты информационной системы.

5.8.2 Процесс определения угроз ИБ должен охватывать все объекты защиты и сегменты в логических и физических границах информационной системы, в которых оператором принимаются и контролируются меры защиты информации. Процесс определения угроз ИБ организуется подразделением оператора, назначенным ответственным за защиту информации в Активе. В случае, если информационная система имеет сегменты, эксплуатируемые разными подразделениями оператора, которые могут самостоятельно принимать и контролировать меры защиты информации, должны быть определены границы ответственности этих подразделений и порядок их взаимодействия в процессе определения угроз ИБ.

5.8.3 Область применения процесса определения угроз ИБ отражается в модели угроз ИБ наряду с областью действия модели угроз, структурно-функциональными характеристиками информационной системы и особенностями ее функционирования.

5.9 Идентификация источников угроз и угроз ИБ

5.9.1 В обобщенном виде угрозы ИБ характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз ИБ.

5.9.2 Важным этапом в процессе определения угроз ИБ является идентификация лиц или событий (явлений), в результате действий (наступления, возникновения) которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в Активе, и возникновение неприемлемых негативных последствий (ущерба). В качестве источников угроз ИБ могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

5.9.3 Источники угроз ИБ являются определяющим фактором при определении угроз ИБ в информационных системах. В процессе определения угроз ИБ подлежат оценке те угрозы, у которых есть источники и источники имеют возможности и условия для реализации угроз ИБ в Активе с заданными структурно-функциональными характеристиками и особенностями ее функционирования.

5.9.4 Источники угроз ИБ могут быть следующих типов:

- антропогенные источники (антропогенные угрозы);
- техногенные источники (техногенные угрозы);
- стихийные источники (угрозы стихийных бедствий, иных природных явлений).

5.9.5 В качестве источников антропогенных угроз ИБ могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в Активе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы ИБ);
- лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы ИБ).

5.9.6 Для информационных систем, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации, в обязательном порядке подлежат оценке техногенные угрозы, связанные с отказами или сбоями в работе технических средств или программного обеспечения. Такие угрозы могут быть обусловлены:

– низким качеством (надежностью) технических, программных или программно-технических средств;

– низким качеством (надежностью) сетей связи и (или) услуг связи; отсутствием или низкой эффективностью систем резервирования или дублирования программно-технических и технических средств;

– низким качеством (надежностью) инженерных систем (кондиционирования, электроснабжения, охранных систем и т.д.);

– низким качеством обслуживания со стороны обслуживающих организаций и лиц.

5.9.7 При определении угроз ИБ оценке подлежат угрозы, связанные со всеми типами источников. Однако в целях создания и эксплуатации адекватной эффективной системы защиты информации в Активе следует, в первую очередь, уделять внимание оценке антропогенных угроз, связанных с несанкционированными (неправомерными) действиями субъектов по нарушению безопасности (конфиденциальности, целостности, доступности) информации, в том числе целенаправленными воздействиями программными (программно-техническими) средствами на информационные системы, осуществляемые в целях нарушения (прекращения) их функционирования (компьютерные атаки).

5.9.8 Также при определении угроз ИБ наряду с угрозами, реализация которых может привести непосредственно к нарушению конфиденциальности, целостности или доступности информации (прямыми угрозами), необходимо выявлять и оценивать угрозы, создающие условия для реализации прямых угроз ИБ (косвенные угрозы). В качестве косвенных угроз ИБ могут рассматриваться угрозы повышения привилегий, исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и иные угрозы ИБ.

5.9.9 В процессе определения угроз ИБ на всех стадиях (этапах) жизненного цикла информационных систем необходимо регулярно проводить идентификацию источников угроз, оценивать их возможности и определять на этой основе угрозы ИБ. Данные о нарушителях и их возможностях по реализации угроз ИБ, полученные при идентификации источников угроз, включаются в модели угроз ИБ.

5.9.10 Для идентификации угроз ИБ в Активе определяются:

– возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз ИБ;

– уязвимости, которые могут использоваться при реализации угроз ИБ (включая специально внедренные программные закладки);

– способы (методы) реализации угроз ИБ;

– объекты информационной системы, на которые направлена угроза ИБ (объекты воздействия);

– результат и последствия от реализации угроз ИБ. Каждая угроза ИБ в Активе описывается (идентифицируется) следующим образом:

$УБИ_j$ = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы].

5.10 Оценка вероятности (возможности) реализации угроз ИБ и степени возможного ущерба

5.10.1 Идентифицированная угроза ИБ подлежит нейтрализации (блокированию), если она является актуальной ($УБИ_j^A$) для информационной системы, то есть в Активе с заданными структурно- функциональными характеристиками и особенностями функционирования существует вероятность (возможность) реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу):

$УБИ_j^A$ = [вероятность (возможность) реализации угрозы (P_j); степень ущерба (X_j)].

5.10.2 Актуальные угрозы ИБ включаются в модель угроз ИБ. Модель угроз ИБ, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

5.11 Мониторинг и переоценка угроз ИБ

5.11.1 Определение угроз ИБ на этапе создания информационной системы позволяет обеспечить формирование требований и внедрение эффективной адекватной системы защиты информации в Активе для угроз, актуальных к моменту ввода в эксплуатацию информационной системы.

5.11.2 В ходе эксплуатации информационной системы оператор, обеспечивая достижение целей и задач информационной системы, может изменять ее базовую конфигурацию, что приводит к изменению структурно-функциональных характеристик информационной системы и применяемых информационных технологий. Также в процессе эксплуатации возможно изменение состава и значимости обрабатываемой информации и особенностей функционирования информационной системы.

5.11.3 В этих условиях процесс определения угроз ИБ должен носить систематический характер. В ходе эксплуатации информационной системы регулярно проводится анализ изменения угроз ИБ, а актуальные угрозы ИБ подлежат периодической переоценке. Периодичность переоценки определяется организацией исходя из особенностей функционирования информационной системы. Рекомендуется пересматривать угрозы ИБ не реже одного раза в год. По результатам анализа проводится уточнение (при необходимости) модели угроз ИБ.

6. Оценка возможностей нарушителей по реализации угроз ИБ

6.1 Целью оценки возможностей нарушителей по реализации угроз ИБ является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы ИБ в Активе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз ИБ.

6.2 Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз ИБ и содержит:

- типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз ИБ;
- цели, которые могут преследовать нарушители каждого вида при реализации угроз ИБ;
- возможные способы реализации угроз ИБ.

6.3 Типы нарушителей

6.3.1 Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам информационной системы, а также анализа возможностей нарушителей по доступу к компонентам информационной системы исходя из структурно-функциональных характеристик и особенностей функционирования информационной системы.

6.3.2 В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа.

6.3.3 Анализ прав доступа проводится, как минимум, в отношении следующих компонент информационной системы:

- устройств ввода/вывода (отображения) информации; беспроводных устройств;
- программных, программно-технических и технических средств обработки информации;
- съемных машинных носителей информации;

– машинных носителей информации, выведенных из эксплуатации; активного (коммутационного) и пассивного оборудования каналов связи; каналов связи, выходящих за пределы контролируемой зоны.

6.3.4 С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

– внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы ИБ из-за границ информационной системы;

– внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

6.3.5 Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором организационные меры по допуску субъектов к работе в Активе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

6.3.6 Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения информационной системы к внешним информационно-телекоммуникационным сетям и (или) имеются линии связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

6.4 Виды и потенциал нарушителей

6.4.1 Угрозы ИБ в Активе могут быть реализованы следующими видами нарушителей:

– специальные службы иностранных государств (блоков государств); террористические, экстремистские группировки;

– преступные группы (криминальные структуры); внешние субъекты (физические лица); конкурирующие организации;

– разработчики, производители, поставщики программных, технических и программно-технических средств;

– лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

– лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

– пользователи информационной системы;

– администраторы информационной системы и администраторы безопасности;

– бывшие работники (пользователи).

6.4.2 Виды нарушителей, характерных для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования, определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации угроз ИБ этими нарушителями.

6.4.3 В качестве возможных целей (мотивации) реализации нарушителями угроз ИБ в Активе могут быть:

– нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

– реализация угроз ИБ по идеологическим или политическим мотивам;

– организация террористического акта;

– причинение имущественного ущерба путем мошенничества или иным преступным путем;

– дискредитация или дестабилизация деятельности органов государственной власти, организаций;

– получение конкурентных преимуществ;

– внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;

– любопытство или желание самореализации;

– выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;

– реализация угроз ИБ из мести;

– реализация угроз ИБ непреднамеренно из-за неосторожности или неквалифицированных действий.

6.4.4 Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач информационной системы, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации. Виды нарушителя и их возможные цели (мотивация) реализации угроз ИБ приведены в таблице 1:

Таблица 1 - Виды нарушителей

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз ИБ
1	Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз ИБ
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
10	Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

6.4.5 При оценке возможностей нарушителей необходимо исходить из условий, что для повышения своих возможностей нарушители 1 вида могут вступать в сговор с нарушителями 3, 4, 6, 7, 8, 9 и 10 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. Нарушители 3 вида могут:

– вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. В случае принятия таких предположений цели (мотивация) и возможности нарушителей подлежат объединению.

– Возможности каждого вида нарушителя по реализации угроз ИБ характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз ИБ в Активе с заданными структурно-функциональными характеристиками и особенностями функционирования.

6.4.6 В зависимости от потенциала, требуемого для реализации угроз ИБ, нарушители подразделяются на:

– нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз ИБ в Активе;

– нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз ИБ в Активе;

– нарушителей, обладающих высоким потенциалом нападения при реализации угроз ИБ в Активе.

6.4.7 Потенциал нарушителей и их возможности приведены в таблице 2.

Таблица 2 - Потенциал нарушителей

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз ИБ
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз ИБ (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в Активе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
3	Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	3 Нарушители с высоким потенциалом Специальные службы иностранных государств (блоков государств) Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз ИБ
			(ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в Активе, об алгоритмах, аппаратных и программных средствах, используемых в Активе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз ИБ с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

6.5 Возможные способы реализации угроз ИБ

6.5.1 Целью определения возможных способов реализации угроз ИБ является формирование предположений о возможных сценариях реализации угроз ИБ, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз ИБ.

6.5.2 Возможные способы реализации угроз ИБ зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

6.5.3 Угрозы ИБ могут быть реализованы нарушителями за счет:

- несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));
- несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

– несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

– несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

– несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

– воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

6.5.4 Действия нарушителя в зависимости от его потенциала при реализации угроз ИБ предусматривают идентификацию и использование уязвимостей в микропрограммном, общесистемном и прикладном программном обеспечении, сетевом оборудовании, применяемых в Активе, а также в организации работ по защите информации и конфигурации информационной системы.

6.5.5 При определении способа реализации угроз ИБ необходимо учитывать то, что угрозы ИБ могут быть реализованы непосредственно за счет доступа к компонентам информационной системы и (или) информации или опосредовано (косвенно) за счет создания условий и (или) средств, обеспечивающих такой доступ, а также за счет доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает. При этом локальной целью нарушителя, не имеющего доступа (прав доступа) к компонентам информационной системы и (или) информации, как правило, является получение доступа к информационной системе (в том числе через внешние сети связи общего пользования) и получение максимально возможных прав и привилегий при таком доступе.

6.5.6 Нарушители могут совершать действия, следствием которых является нарушение безопасности информации, преднамеренно (преднамеренные угрозы ИБ) или случайно (непреднамеренные угрозы ИБ).

6.5.7 Преднамеренные действия нарушителей могут заключаться в реализации целенаправленных или нецеленаправленных угроз ИБ.

6.5.8 Целенаправленная угроза ИБ направлена на интересующую нарушителя информационную систему с заранее известными ему структурно-функциональными характеристиками и особенностями функционирования. Целенаправленная угроза ИБ адаптирована к структурно-функциональным характеристикам информационной системы. При подготовке и реализации целенаправленных угроз ИБ нарушитель может использовать методы социальной инженерии, которые позволяют ему изучить поведение пользователей и их реакцию на поступающие к ним внешние данные.

6.5.9 Нецеленаправленная («веерная») угроза ИБ не ориентирована на конкретную информационную систему. Целями такой угрозы могут являться несанкционированный доступ, перехват управления или воздействие на как можно большее количество информационных систем. В данном случае нарушителю заранее не известны структурно-функциональные характеристики и условия функционирования информационной системы.

6.5.10 Реализация преднамеренных угроз ИБ, как правило, включает:

– Сбор информации об информационной системе, ее структурно-функциональных характеристиках, условиях функционирования;

– выбор (разработка, приобретение) методов и средств, используемых для реализации угроз ИБ в Активе с заданными структурно-функциональными характеристиками и условиями функционирования;

– непосредственная реализация угроз ИБ в Активе (проникновение в информационную систему, закрепление в Активе, реализация неправомерных действий);

– устранение признаков и следов неправомерных действий в Активе.

6.5.11 В зависимости от целей и потенциала нарушителя на каждом из этапов могут эксплуатироваться одна или несколько уязвимостей информационной системы.

6.5.12 При определении возможных способов реализации угроз ИБ необходимо исходить из следующих условий:

– нарушитель может действовать один или в составе группы нарушителей;

– в отношении информационной системы внешний нарушитель может действовать совместно с внутренним нарушителем;

– угрозы могут быть реализованы в любое время и в любой точке информационной системы (на любом узле или хосте);

– для достижения своей цели нарушитель выбирает наиболее слабое звено информационной системы.

6.5.13 Возможные способы реализации угроз ИБ, определенные на основе настоящего раздела, включаются в модель угроз ИБ.

7. Определение актуальных угроз ИБ

7.1 Угроза ИБ является актуальной ($УБИ_j^A$), если для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности информации.

7.2 В качестве показателя актуальности угрозы ИБ ($УБИ_j^A$) принимается двухкомпонентный вектор, первый компонент которого характеризует вероятность реализации угрозы (P_j), а второй – степень возможного ущерба в случае ее реализации (X_j)

$УБИ_j^A$ = [вероятность реализации угрозы (P_j); степень ущерба (X_j)],

где P_j определятся на основе анализа статистических данных о частоте реализации угроз ИБ (возникновении инцидентов безопасности) в Активе и (или) однотипных информационных системах, а X_j определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

7.3 При отсутствии статистических данных о реализации угроз ИБ (возникновении инцидентов безопасности) в Активе и (или) однотипных информационных системах, актуальность угрозы ИБ определяется на основе оценки возможности реализации угрозы ИБ (Y_j)

$УБИj^A$ = [возможность реализации угрозы (Y_j); степень ущерба (X_j)],

где Y_j определятся на основе оценки уровня защищенности информационной системы и потенциала нарушителя, требуемого для реализации угрозы безопасности. X_j также определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

7.4 Актуальность угроз ИБ определяется в отношении угроз, для которых экспертным методом определено, что:

– возможности (потенциал) нарушителя достаточны для реализации угрозы ИБ;

– в Активе могут иметься потенциальные уязвимости, которые могут быть использованы при реализации j-ой угрозы ИБ;

– структурно-функциональные характеристики и особенности функционирования информационной системы не исключают возможности применения способов, необходимых для реализации j-ой угрозы ИБ (существует сценарий реализации угрозы безопасности);

– реализация угрозы ИБ приведет к нарушению конфиденциальности, целостности или доступности информации, в результате которого возможно возникновение неприемлемых негативных последствий (ущерба).

7.5 В качестве исходных данных об угрозах ИБ и их характеристиках используется банк данных угроз ИБ, сформированный и поддерживаемый ФСТЭК России, а также базовые и типовые модели угроз ИБ, разрабатываемые ФСТЭК России для различных классов и типов информационных систем.

7.6 Для определения угроз ИБ могут использоваться иные источники, в том числе опубликованные в общедоступных источниках данные об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, а также результаты специально проведенных исследований по выявлению угроз ИБ. В этом случае потенциал нарушителя, возможные уязвимости, способы реализации угрозы ИБ и последствия от ее реализации определяются для каждой угрозы ИБ.

7.7 Оценка вероятности (возможности) реализации угрозы ИБ ИБ

7.7.1 Под вероятностью реализации угрозы ИБ понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация j-ой угрозы ИБ в Активе с заданными структурно-функциональными характеристиками и особенностями функционирования. Вводятся три вербальные градации этого показателя:

- низкая вероятность – отсутствуют объективные предпосылки к реализации j-ой угрозы ИБ, отсутствует требуемая статистика по фактам реализации j-ой угрозы ИБ (возникновения инцидентов безопасности), отсутствует мотивация для реализации j-ой угрозы, возможная частота реализации j-ой угрозы не превышает 1 раза в 5 лет;
- средняя вероятность – существуют предпосылки к реализации j-ой угрозы ИБ, зафиксированы случаи реализации j-ой угрозы ИБ (возникновения инцидентов безопасности) или имеется иная информация, указывающая на возможность реализации j-ой угрозы ИБ, существуют признаки наличия у нарушителя мотивации для реализации такой угрозы, возможная частота реализации j-ой угрозы не превышает 1 раза в год;
- высокая вероятность – существуют объективные предпосылки к реализации j-ой угрозы ИБ, существует достоверная статистика реализации j-ой угрозы ИБ (возникновения инцидентов безопасности) или имеется иная информация, указывающая на высокую возможность реализации j-ой угрозы ИБ, у нарушителя имеются
- мотивы для реализации j-ой угрозы, частота реализации j-ой угрозы – чаще 1 раза в год.

7.7.2 В случае отсутствия требуемых данных для оценки вероятности реализации угрозы ИБ или наличия сомнений в объективности экспертных оценок при определении вербальных градаций вероятности реализации угроз ИБ, актуальность j-ой угрозы ИБ определяется на основе оценки возможности ее реализации (Y_j).

7.7.3 Возможность реализации j-ой угрозы ИБ (Y_j) оценивается исходя из уровня защищенности информационной системы (Y_1) и потенциала нарушителя (Y_2), необходимого для реализации этой угрозы ИБ в Активе с заданными структурно-функциональными характеристиками и особенностями функционирования:

Y_j = [уровень защищенности (Y_1); потенциал нарушителя (Y_2)].

7.7.4 При определении угроз ИБ на этапе создания информационной системы в случае, когда меры защиты информации не реализованы или не проведена оценка их достаточности и эффективности, оценка возможности реализации j-ой угрозы ИБ (Yj) проводится относительно уровня проектной защищенности информационной системы ($Y_{1П}$):

Y_j = [уровень проектной защищенности ($Y_{1П}$); потенциал нарушителя (Y_2)].

7.7.5 Под уровнем проектной защищенности ($Y_{1П}$) понимается исходная защищенность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности ($Y_{1П}$) определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице 3.

Таблица 3 - Показатели, характеризующие проектную защищенность информационной системы

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы ($Y_{1П}$)		
	Высокий	Средний	Низкий
1. По структуре информационной системы:			
Автономное автоматизированное рабочее место	+		
Локальная информационная система		+	
Распределенная информационная система			+
2. По используемым информационным технологиям:			
Системы на основе виртуализации			+
Системы, реализующие «облачные вычисления»			+
Системы с мобильными устройствами			+
Системы с технологиями беспроводного доступа			+
Грид-системы			+
Суперкомпьютерные системы		+	
3. По архитектуре информационной системы:			
Системы на основе «тонкого клиента»	+		
Системы на основе одноранговой сети		+	
Файл-серверные системы			+
Центры обработки данных			+
Системы с удаленным доступом пользователей			+
Использование разных типов операционных систем (гетерогенность среды)		+	
Использование прикладных программ, независимых от операционных систем		+	
Использование выделенных каналов связи		+	
4. По наличию (отсутствию) взаимосвязей с иными информационными системами:			
Взаимодействующая с системами			+
Невзаимодействующая с системами		+	
5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования			
Подключенная			+
Подключенная через выделенную инфраструктуру (gov.ru или иную)		+	
Неподключенная	+		
6. По размещению технических средств:			
Расположенные в пределах одной контролируемой зоны	+		
Расположенные в пределах нескольких контролируемых зон		+	
Расположенные вне контролируемой зоны			+
7. По режимам обработки информации в Активе			
Многопользовательский			+
Однопользовательский	+		
8. По режимам разграничения прав доступа			
Без разграничения			+

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы ($Y_{1П}$)		
	Высокий	Средний	Низкий
С разграничением		+	
9. По режимам разделения функций по управлению информационной системой			
Без разделения			+
Выделение рабочих мест для администрирования в отдельный домен		+	
Использование различных сетевых адресов		+	
Использование выделенных каналов для администрирования		+	
10. По подходам к сегментированию информационной системы:			
Без сегментирования;			+
С сегментированием		+	

7.7.6 В ходе создания информационной системы уровень ее проектной защищенности ($Y_{1П}$) определяется следующим образом:

7.7.6.1 Информационная система имеет высокий уровень проектной защищенности ($Y_{1П}$), если не менее 80% характеристик информационной системы соответствуют уровню «высокий» (суммируются положительные решения по второму столбцу, соответствующему высокому уровню защищенности), а остальные среднему уровню защищенности (положительные решения по третьему столбцу);

7.7.6.2 Информационная система имеет средний уровень проектной защищенности ($Y_{1П}$), если не выполняются условия по пункту 7.7.6.1 и не менее 90% характеристик информационной системы соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по третьему столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные низкому уровню защищенности;

7.7.6.3 Информационная система имеет низкий уровень проектной защищенности ($Y_{1П}$), если не выполняются условия по пунктам 7.7.6.1 и 7.7.6.2.

7.7.7 До ввода в эксплуатацию информационной системы должны быть реализованы меры защиты информации, направленные на блокирование (нейтрализацию) актуальных угроз ИБ. Таким образом, ввод в эксплуатацию информационной системы осуществляется при условии достижения высокого уровня исходной защищенности информационной системы от нарушителя с заданным потенциалом.

7.7.8 Вместе с тем, в ходе эксплуатации информационной системы возможно появление новых уязвимостей, повышение потенциала нарушителя, изменение структурно-функциональных характеристик, значимости обрабатываемой информации, особенностей функционирования информационной системы и других условий, приводящих к возникновению новых угроз ИБ, которые могут существенно снизить уровень проектной защищенности информационной системы. В этом случае для поддержания уровня защищенности информационной системы в ходе эксплуатации должен проводиться регулярный анализ изменения угроз ИБ, а актуальные угрозы ИБ подлежат периодической переоценке.

7.7.9 В ходе эксплуатации информационной системы уровень ее защищенности (Y_1) определяется следующим образом:

7.7.9.1 В информационной системе обеспечивается высокий уровень защищенности (Y_1), если в ходе эксплуатации информационной системы не появились дополнительные угрозы ИБ или в отношении появившихся дополнительных угроз ИБ с высокой оперативностью («за минуты») могут быть приняты меры защиты информации, нейтрализующие эти угрозы.

7.7.9.2 В информационной системе обеспечивается средний уровень защищенности (Y_1), если в ходе эксплуатации информационной системы появились дополнительные угрозы ИБ и в отношении них оперативно («за часы») могут быть приняты меры защиты информации, нейтрализующие эти угрозы.

7.7.9.3 В информационной системе обеспечивается низкий уровень защищенности (Y_1), если в ходе эксплуатации информационной системы появились дополнительные угрозы ИБ и в отношении них не могут быть с высокой оперативностью или оперативно приняты меры защиты информации, нейтрализующие эти угрозы

7.7.10 Потенциал, требуемый нарушителю для реализации j-ой угрозы ИБ, может быть базовым (низким), базовым повышенным (средним) или высоким. Значение потенциала нарушителя (Y_2) для j-ой угрозы ИБ определяется на основе данных, приведенных в банке данных угроз ИБ ФСТЭК России, а также в базовых и типовых моделях угроз ИБ, разрабатываемых ФСТЭК России для информационных систем различных классов и типов. В случае отсутствия информации о потенциале нарушителя для реализации j-ой угрозы безопасности значение потенциала (Y_2) определяется в соответствии с Приложением № 2 к Методики.

7.7.11 Возможность реализации j-ой угрозы ИБ (Y_j) в зависимости от уровня защищенности информационной системы (Y_1/$Y_{1П}$) и потенциала нарушителя (Y_2) определяется как высокая, средняя или низкая в соответствии с таблицей 4.

Таблица 4 – Возможность реализации угрозы ИБ

Уровень защищенности (Y_1/$Y_{1П}$) / **Потенциал нарушителя (Y_2)**	**Высокий**	**Средний**	**Низкий**
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый повышенный (средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

7.8 Оценка степени возможного ущерба от реализации угрозы ИБ

7.8.1 Для оценки степени возможного ущерба от реализации угрозы ИБ определяются возможный результат реализации угрозы ИБ в информационной системе, вид ущерба, к которому может привести реализация угрозы ИБ, степень последствий от реализации угрозы ИБ для каждого вида ущерба.

7.8.2 В качестве результата реализации угрозы ИБ рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

7.8.3 Непосредственное воздействие на конфиденциальность, целостность, доступность информации возможно в результате реализации прямой угрозы ИБ. В этом случае объектами воздействия угрозы являются непосредственно информация и (или) иные объекты защиты информационной системы или обеспечивающей инфраструктуры, которые обеспечивают получение, обработку, хранение, передачу, уничтожение информации в информационной системе, в результате доступа к которым или воздействия, на которые возможно воздействие на конфиденциальность, целостность или доступность информации.

7.8.4 Опосредованное воздействие на конфиденциальность, целостность, доступность информации рассматривается в результате реализации косвенных угроз ИБ. Реализация косвенных угроз ИБ не приводит непосредственно к воздействию на конфиденциальность, целостность, доступность информации, но создает условия для реализации одной или нескольких прямых угроз ИБ, позволяющих реализовать такое воздействие. В этом случае в качестве результата реализации косвенной угрозы

необходимо рассматривать результаты реализации всех прямых угроз ИБ, которые возможно реализовать в случае реализации данной косвенной угрозы.

7.8.5 Результат реализации угрозы ИБ определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии с таблицей 5. При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна, иные установленные законодательством Российской Федерации виды информации) воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации (k, …, m), содержащейся в информационной системе.

Таблица 5 - Результат реализации угрозы ИБ

Свойство ИБ	Результат реализации угрозы ИБ	
	Не оказывает воздействия	Оказывает воздействие
Конфиденциальность $X^{К}_{k_1}$	В результате реализации угрозы ИБ отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы ИБ возможны неправомерный доступ, копирование, предоставление или распространение
Целостность $X^{Ц}_{k_1}$	В результате реализации угрозы ИБ отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы ИБ возможно уничтожение или модифицирование информации
Доступность $X^{Д}_{k_1}$	В результате реализации угрозы ИБ отсутствует возможность блокирования информации	В результате реализации угрозы ИБ возможно блокирование информации

7.8.6 При определении степени возможного ущерба необходимо исходить из того, что в зависимости от целей и задач, решаемых информационной системой, видов обрабатываемой информации, воздействие на конфиденциальность, целостность или доступность каждого вида информации, содержащейся в информационной системе, может привести к различным видам ущерба. При этом для разных обладателей информации и операторов будут характерны разные виды ущерба.

7.8.7 Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в таблице 6.

Таблица 6 - Виды ущерба и негативных последствий

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	Снижение, как минимум, одного экономического показателя. Потеря (кража) финансовых средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Другие прямые или косвенные финансовые потери
Социальный	Создание предпосылок для нанесения вреда здоровью граждан.

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
	Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан. Организация пикетов, забастовок, митингов и других акций. Увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Невозможность (прерывание) предоставления социальных услуг (сервисов). Другие последствия, приводящие к нарастанию социальной напряженности в обществе
Политический	Создание предпосылок к обострению отношений в международных отношениях. Срыв двусторонних (многосторонних) контактов с зарубежными партнерами. Неспособность выполнения международных (двусторонних) договорных обязательств. Невозможность заключения международных (двусторонних) договоров, соглашений. Создание предпосылок к внутриполитическому кризису. Нарушение выборного процесса. Другие последствия во внутриполитической и внешнеполитической областях деятельности
Репутационный	Нарушение законодательных и подзаконных актов. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Неспособность выполнения договорных обязательств. Другие последствия, приводящие к нарушению репутации
Ущерб в области обороны, безопасности и правопорядка	Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка. Нарушение общественного правопорядка. Неблагоприятное влияние на обеспечение общественного правопорядка. Возможность потери или снижения уровня контроля за общественным правопорядком. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка
Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных
Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений.

Вид ущерба	Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации
	Простой информационной системы или сегмента информационной системы Другие последствия, приводящие к нарушению технологии обработки информации

7.8.8 Указанные виды ущерба могут дополняться другими видами в зависимости от целей и задач, решаемых информационной системой, а также вида обрабатываемой в ней информации.

7.8.9 Степень возможного ущерба от реализации угрозы ИБ определяется степенью негативных последствий от нарушения конфиденциальности, целостности или доступности каждого вида информации, содержащейся в информационной системе.

7.8.10 Степень негативных последствий от нарушения конфиденциальности, целостности или доступности информации определяется для каждого вида ущерба, зависит от целей и задач, решаемых информационной системой, и может иметь разные значения для разных обладателей информации и операторов. В качестве единой шкалы измерения степени негативных последствий принимаются значения «незначительные», «умеренные» и «существенные» негативные последствия. Каждым оператором определяется в указанной единой шкале измерений степень негативных последствий от нарушения конфиденциальности, целостности или доступности информации применительно ко всем целям и задачам, решаемым информационной системой.

7.8.11 Степень возможного ущерба определяется экспертным методом в соответствии с таблицей 7.

Таблица 7 - Степени ущерба

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них
Средняя	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

7.8.12 При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна и иные установленные законодательством Российской Федерации виды информации) степень возможного ущерба определяется отдельно для каждого вида информации (k, …, m), обрабатываемой в информационной системе, применительно к каждому виду ущерба. Итоговая степень возможного ущерба устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации применительно к каждому виду ущерба.

$$X_k = \max_i(X_k^i)\,;\, i = К, Ц, Д.$$

7.9 Определение актуальности угрозы ИБ

7.9.1 Решение об актуальности угрозы ИБ $УБИ_j^A$ для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей 8.

Таблица 8 – Определение актуальности угрозы ИБ

Вероятность (возможность) реализации	Степень возможного ущерба (X_j)		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

8. Требования к модели угроз ИБ

8.1 Структура модели угроз ИБ приведена в Приложении № 3 к Методике.

9. Порядок пересмотра Методики

9.1 При возникновении необходимости в Методику вносятся изменения.

9.2 ДИБ осуществляет пересмотр Методики не реже одного раз в год.

10. Контроль

10.1 Контроль за соблюдением правил разработки моделей угроз информационной безопасности осуществляется ДИБ.

Банк данных угроз ФСТЭК

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
001	Угроза автоматического распространения вредоносного кода в грид-системе	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы	1	1	1
002	Угроза агрегирования данных, передаваемых в грид-системе	Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: – сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; – привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы	Внешний нарушитель со средним потенциалом	Сетевой трафик	1	0	0
003	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	1	1	0
004	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	0	1	0
005	Угроза внедрения вредоносного кода в BIOS	Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
006	Угроза внедрения кода или данных	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. Данная угроза обусловлена: – наличием уязвимостей программного обеспечения; – слабостями мер антивирусной защиты и разграничения доступа; – наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств). – Реализация данной угрозы возможна: – в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; – при наличии у него привилегий установки программного обеспечения; – в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)	Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
007	Угроза воздействия на программы с высокими привилегиями	Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик	1	1	0
008	Угроза восстановления аутентификационной информации	Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: – время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; – восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). – Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	1	0	0
009	Угроза восстановления предыдущей уязвимой версии BIOS	Угроза заключается в возможности осуществления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке):	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию					
010	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины	1	1	1
011	Угроза деавторизации санкционированного клиента беспроводной сети	Угроза заключается в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети. Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных – сведения о MAC-адресах беспроводных клиентов доступны всем участникам сетевого взаимодействия. Реализация данной угрозы возможна при условии подключения нарушителем к беспроводной сети устройства, MAC-адрес которого будет полностью совпадать с MAC-адресом дискредитируемого санкционированного клиента	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел	0	0	1
012	Угроза деструктивного изменения конфигурации/среды окружения программ	Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	1	1	1
013	Угроза деструктивного использования декларированного функционала BIOS	Угроза заключается в возможности неправомерного использования декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения BIOS/UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки целостности памяти, программного обеспечения управления RAID-контроллером и т.п.). Реализации данной угрозы может способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	0	1	0
014	Угроза длительного удержания вычислительных ресурсов пользователями	Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя		программное обеспечение, сетевое программное обеспечение, сетевой трафик			
015	Угроза доступа к защищаемым файлам с использованием обходного пути	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы. Реализация данной угрозы возможна при условиях: – наличие у нарушителя прав доступа к некоторым объектам файловой системы; – отсутствие проверки вводимых пользователем данных; – наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы	1	0	0
016	Угроза доступа к локальным файлам сервера при помощи URL	Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	1	0	0
017	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов: отсутствием проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	1	0	1
018	Угроза загрузки нештатной операционной системы	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	1	1
019	Угроза заражения DNS-кеша	Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера.	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу					
020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг	Внутренний нарушитель с низким потенциалом	Облачная система, виртуальная машина	1	1	1
021	Угроза злоупотребления доверием потребителей облачных услуг	Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки)	Внешний нарушитель с низким потенциалом	Облачная система	1	1	0
022	Угроза избыточного выделения оперативной памяти	Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	0	0	1
023	Угроза изменения компонентов системы	Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе	Внутренний нарушитель с низким потенциалом	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	0	1	1
024	Угроза изменения режимов работы аппаратных элементов компьютера	Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера;	Внутренний нарушитель с высоким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки BIOS/UEFI					
025	Угроза изменения системных и глобальных переменных	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения	Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
026	Угроза искажения XML-схемы	Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями механизма сетевого взаимодействия открытых систем. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к сетевому трафику, передаваемому между клиентом и сервером и отсутствии проверки целостности XML-схемы со стороны дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	0	1	1
027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение	0	1	0
028	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: – возможности ввода произвольных данных в адресную строку; – сведений о пути к защищаемому ресурсу; – возможности изменения интерфейса ввода входных данных	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	1	0	0
029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Угроза заключается в возможности существенного снижения производительности вычислительного поля суперкомпьютера и эффективности выполнения на нём текущих параллельных вычислений из-за потребления вычислительных ресурсов суперкомпьютера «паразитными» процессами («процессами-потомками» предыдущих заданий или процессами, запущенными вредоносным программным обеспечением).	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением. Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии					
030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: – наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; – успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	1	1	1
031	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	0	0
032	Угроза использования поддельных цифровых подписей BIOS	Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений	Внешний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	0	1	0
033	Угроза использования слабостей кодирования входных данных	Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: – дискредитируемая система принимает входные данные от нарушителя; – нарушитель обладает возможностью управления одним или несколькими параметрами входных данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	1	0	0
035	Угроза использования слабых криптографических алгоритмов BIOS	Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы	Внешний нарушитель с высоким потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	1	1
036	Угроза исследования механизмов работы программы	Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: – наличия у нарушителя доступа к исходным файлам программы; – наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	1	0	1
037	Угроза исследования приложения через отчёты об ошибках	Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	1	0	0
038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Угроза заключается в возможности временного возникновения состояния типа «отказ в обслуживании» у хранилища больших данных. Данная угроза обусловлена постоянным трудно контролируемым заполнением занятого дискового пространства за счёт данных, непрерывно поступающих из различных информационных источников, и слабостями технологий доступа и хранения информации в хранилищах больших данных. Реализация данной угрозы возможна при условии мгновенного (текущего) превышения скорости передачи данных над скоростью их сохранения (в силу недостаточности пропускной способности канала связи или скорости выделения свободного пространства и сохранения на него поступающих данных) или при условии временного отсутствия свободного места в хранилище (в силу некорректного управления хранилищем или в результате осуществления нарушителем деструктивного программного воздействия на механизм контроля за заполнением хранилища путём изменения параметров или логики его работы)	Внутренний нарушитель с низким потенциалом	Информационная система	0	0	1
039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей.	Внешний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI	0	1	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей					
040	Угроза конфликта юрисдикций различных стран	Угроза заключается в возможности отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства стран, резиденты которых участвуют в оказании облачных услуг. Данная угроза обусловлена тем, что в зависимости от особенностей законодательства различных стран, резиденты которых участвуют в оказании облачных услуг, при обеспечении информационной безопасности могут использоваться правовые меры различных юрисдикций. Реализация данной угрозы возможна при условии того, что на обеспечение информационной безопасности в ходе оказания облачных услуг накладываются правовые меры различных юрисдикций, противоречащих друг другу в ряде вопросов	Внешний нарушитель с низким потенциалом	Облачная система	0	0	1
041	Угроза межсайтового скриптинга	Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	1	1
042	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	1	1	1
043	Угроза нарушения доступности облачного сервера	Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, облачный сервер	0	0	1
044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальная машина, гипервизор	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы					
045	Угроза нарушения изоляции среды исполнения BIOS	Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: – со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; – со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	1	1	1
046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя	1	0	1
047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). Данная угроза обусловлена слабостью технологий грид-вычислений – производительность грид-системы имеет сильную зависимость от загруженности каналов связи, что является следствием максимальной территориальной распределённости вычислительного модуля грид-системы среди всех типов информационных систем. Реализация данной угрозы возможна при условии недостаточного контроля за состоянием отдельных узлов грид-системы со стороны диспетчера задач грид-системы	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Грид-система, сетевой трафик	0	0	1
048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: – к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов; – к нарушению целостности программ, установленных на виртуальных машинах; – к нарушению доступности ресурсов виртуальных машин; – к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы)	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина	1	1	1
049	Угроза нарушения целостности данных кеша	Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)					
050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультиформатной информации в хранилищах больших данных. Реализация данной угрозы возможна при условии, что дополнительная служебная информация о данных по какой-либо причине не соответствует их фактическому содержимому, или в хранилище больших данных не реализованы методы обработки данных получаемого формата	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные	0	1	0
051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания («ждущего режима работы», «гибернации» и др.)	Внутренний нарушитель с низким потенциалом	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр	0	1	1
052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг	Внешний нарушитель с низким потенциалом	Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение	0	1	1
053	Угроза невозможности управления правами пользователей BIOS	Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами. Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	1	1
054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей.	Внешний нарушитель с низким потенциалом	Информационная система, сервер, носитель информации, метаданные, объекты файловой системы	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.					
055	Угроза незащищённого администрирования облачных услуг	Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, функционирующие в облачной среде, путём перехвата управления над облачной инфраструктурой через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями облачных услуг данных (в том числе аутентификационных данных), а также уязвимостями небезопасных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, рабочая станция, сетевое программное обеспечение	1	1	1
056	Угроза некачественного переноса инфраструктуры в облако	Угроза заключается в возможности снижения реального уровня защищённости иммигрирующей в облако информационной системы из-за ошибок, допущенных при миграции в ходе преобразования её реальной инфраструктуры в облачную. Данная угроза обусловлена тем, что преобразование даже части инфраструктуры информационной системы в облачную зачастую требует проведения серьёзных изменений в такой инфраструктуре (например, в политиках безопасности и организации сетевого обмена данными). Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при осуществлении переноса информационной системы в облако	Внешний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, облачная система	1	1	1
057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. Данная угроза обусловлена осуществлением дублирования (дву- или многократного) данных на различных вычислительных узлах, входящих в состав хранилища больших данных, с целью повышения скорости доступа к этим данным при большом количестве запросов чтения/записи. При этом данная операция является внутренней функцией и «непрозрачна» для конечных пользователей и администраторов хранилища больших данных. Реализация данной угрозы возможна при условии недостаточности мер по контролю за автоматически создаваемыми копиями информации, применяемых в хранилище больших данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные	1	0	0
058	Угроза неконтролируемого роста числа виртуальных машин	Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура	0	0	1
059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сервер	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями					
060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Угроза заключается в возможности удаления из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора. Данная угроза обусловлена слабостями механизма автоматического удаления данных, не отвечающих определённым требованиям (предельный «срок жизни» в хранилище, конечная несогласованность с другими данными, создание копии в другом месте и т.п.). Реализация данной угрозы возможна при условии недостаточности реализованных в хранилище больших данных мер по контролю за автоматическим удалением данных	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные, защищаемые данные	0	1	1
061	Угроза некорректного задания структуры данных транзакции	Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом	Внутренний нарушитель со средним потенциалом	Сетевой трафик, база данных, сетевое программное обеспечение	0	1	1
062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	0	0
063	Угроза некорректного использования функционала программного обеспечения	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	1	1	1
064	Угроза некорректной реализации политики лицензирования в облаке	Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	0	0	1
065	Угроза неопределённости в распределении ответственности между ролями в облаке	Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности. Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки облачной инфраструктуры и т. п.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Возможность реализации данной угрозы повышается в случае использования облачных услуг, предоставляемых другими поставщиками (т.е. в случае использования схемы оказания облачных услуг с участием посредников)					
066	Угроза неопределённости ответственности за обеспечение безопасности облака	Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности	Внешний нарушитель с низким потенциалом	Облачная система	1	1	1
067	Угроза неправомерного ознакомления с защищаемой информацией	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.	Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, носители информации, объекты файловой системы	1	0	0
068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд API, используемого программным обеспечением. Реализация данной угрозы возможна в условиях наличия у нарушителя доступа к API и отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	1	1	1
069	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	Внешний нарушитель с низким потенциалом	Сетевой трафик	1	1	0
070	Угроза непрерывной модернизации облачной инфраструктуры	Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться таковой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)	Внутренний нарушитель со средним потенциалом	Облачная инфраструктура	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
071	Угроза несанкционированного восстановления удалённой защищаемой информации	Угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: – удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); – технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; – информация не хранилась в криптографически преобразованном виде	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Машинный носитель информации	1	0	0
072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Угроза заключается в возможности внедрения в BIOS/UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в BIOS/UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостями механизма обновления BIOS/UEFI, приводящими к переполнению буфера. Реализация данной угрозы возможна в одном из следующих условий: выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	1	1	1
073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства	1	1	1
074	Угроза несанкционированного доступа к аутентификационной информации	Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	1	0	0
075	Угроза несанкционированного доступа к виртуальным каналам передачи	Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных).	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации					
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: – наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; – наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Гипервизор	0	0	1
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сервер, рабочая станция, виртуальная машина, гипервизор, машинный носитель информации, метаданные	0	1	1
078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина	1	1	1
079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина	1	1	1
080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Виртуальные устройства хранения,	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
	виртуальной и (или) физической сети	осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации		обработки и передачи данных			
081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Угроза заключается в возможности выполнения нарушителем сетевого входа на узел грид-системы с правами одной из учётных записей, соответствующей программным процессам системы управления заданиями, с последующим получением доступа к закрытой части криптографических сертификатов, используемых для установления связи в грид-системе. Данная угроза обусловлена наличием уязвимостей в клиенте грид-системы (клиентского программного обеспечения, устанавливаемого в узлах грид-системы), эксплуатация которых позволяет нарушителю осуществлять операции чтения и записи в объектах локальной файловой системы компьютера, отправку сигналов программным процессам (включая сигналы прекращения работы), операции чтения и записи в память программных процессов, соответствующих связующему программному обеспечению и грид-заданиям, открытия сетевых соединений в локальных и внешних узлах грид-системы. Реализация данной угрозы возможна при условии внедрения вредоносного программного кода в систему управления заданиями. Фактически наличие в узле грид-системы неизвестного его владельцу программного обеспечения (клиента грид-системы), проводящего неизвестные вычисления, является «черным ящиком», через который (путём эксплуатации уязвимостей или программных закладок) нарушитель может осуществить противоправные действия по отношению к хранящейся в узле грид-системы защищаемой информации (личной информации владельца узла)	Внешний нарушитель со средним потенциалом	Узлы грид-системы	1	1	1
082	Угроза несанкционированного доступа к сегментам вычислительного поля	Угроза заключается в возможности осуществления несанкционированного доступа нарушителя к исходным данным, промежуточным и окончательным результатам расчётов других пользователей суперкомпьютера, а также случайное или преднамеренное деструктивное воздействие процессов решения одних задач на процессы и результаты решения других вычислительных задач. Данная угроза обусловлена слабостями механизма разграничения доступа субъектов к сегментам вычислительных полей суперкомпьютера. Реализация данной угрозы возможна при выполнении задач различных пользователей суперкомпьютера на одном вычислительном поле суперкомпьютера	Внутренний нарушитель со средним потенциалом	Вычислительный узел суперкомпьютера	1	1	0
083	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2), используемых для авторизации пользователей при подключении к точке беспроводного доступа. Реализация данной угрозы возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации/аутентификации беспроводных сетей, а также нахождения в точке приёма сигналов дискредитируемой беспроводной сети	Внешний нарушитель с низким потенциалом	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	1	0	0
084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальные устройства хранения данных, виртуальные диски	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)					
085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, объекты файловой системы	1	0	0
086	Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	0	1	1
087	Угроза несанкционированного использования привилегированных функций BIOS	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI	1	1	1
088	Угроза несанкционированного копирования защищаемой информации	Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, машинный носитель информации	1	0	0
089	Угроза несанкционированного редактирования реестра	Угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, использующее реестр, реестр	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
090	Угроза несанкционированного создания учётной записи пользователя	Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	1	1	1
091	Угроза несанкционированного удаления защищаемой информации	Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Метаданные, объекты файловой системы, реестр	0	0	1
092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; наличия подключения системы к сетям общего пользования (сети Интернет)	Внешний нарушитель с высоким потенциалом	Информационная система, аппаратное обеспечение	1	1	1
093	Угроза несанкционированного управления буфером	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
094	Угроза несанкционированного управления синхронизацией и состоянием	Угроза заключается в возможности изменения нарушителем последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния информационной системы (например, текущих значений глобальных переменных, наличия запущенных процессов и др.), или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.). Данная угроза основана на слабостях механизма управления синхронизацией и состоянием, позволяющих нарушителю вносить изменения в его работу в определённые промежутки времени, или отсутствии механизмов аутентификации и авторизации. Реализация данной угрозы возможна при условии наличия у нарушителя возможности:	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		– контролировать состояние дискредитируемого приложения (этапы выполнения алгоритма) или промышленных роботов; – отслеживать моменты времени, когда дискредитируемое приложение временно прерывает свою работу с глобальными данными; – выполнить деструктивные действия в определённые моменты времени (например, внести изменения в файл с данными или изменить содержимое ячейки памяти)					
095	Угроза несанкционированного управления указателями	Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённости облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, облачная система	1	1	1
097	Угроза несогласованности правил доступа к большим данным	Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)	Внутренний нарушитель с низким потенциалом	Хранилище больших данных	1	0	1
098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0
099	Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
100	Угроза обхода некорректно настроенных механизмов аутентификации	Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). Данная угроза обусловлена в случае некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных. Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение	1	1	1
101	Угроза общедоступности облачной инфраструктуры	Угроза заключается в возможности осуществления несанкционированного доступа к защищаемой информации одного потребителя облачных услуг со стороны другого. Данная угроза обусловлена тем, что из-за особенностей облачных технологий потребителям облачных услуг приходится совместно использовать одну и ту же облачную инфраструктуру. Реализация данной угрозы возможна в случае допущения ошибок при разделении элементов облачной инфраструктуры между потребителями облачных услуг, а также при изоляции их ресурсов и обособлении данных друг от друга	Внешний нарушитель со средним потенциалом	Объекты файловой системы, аппаратное обеспечение, облачный сервер	1	1	1
102	Угроза опосредованного управления группой программ через совместно используемые данные	Угроза заключается в возможности опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные, файлы конфигурации и др.). Данная угроза обусловлена наличием слабостей в механизме контроля внесённых изменений в общие данные каждой из программ в группе. Реализация данной угрозы возможна в случае успешного перехвата нарушителем управления над одной из программ в группе программ, использующих общие данные	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	0	1	1
103	Угроза определения типов объектов защиты	Угроза заключается в возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (данный метод известен как «fingerprinting», с англ. «дактилоскопия»). Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз. Данная угроза обусловлена ошибками в параметрах конфигурации средств межсетевого экранирования, а также с отсутствием механизмов контроля входных и выходных данных. Реализация данной угрозы возможна в случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией дискредитируемой системы (документация на программные средства, стандарты передачи данных, спецификации и т.п.)	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0
104	Угроза определения топологии вычислительной сети	Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика). Реализация данной угрозы возможна в случае наличия у нарушителя возможности подключения к исследуемой вычислительной сети и наличием специализированного программного обеспечения, реализующего функцию анализа сетевого трафика	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0
105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Угроза заключается в возможности отказа хранилищем больших данных в приёме входных данных неизвестного формата от легального пользователя. Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных. Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата	Внутренний нарушитель с низким потенциалом	Хранилище больших данных, метаданные	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Угроза заключается в возможности значительного замедления работы терминальных сессий всех пользователей суперкомпьютера, вплоть до достижения всем суперкомпьютером состояния «отказ в обслуживании» при превышении максимально достижимой нагрузки на параллельную файловую систему суперкомпьютера. Данная угроза обусловлена значительным повышением числа и объёма сохраняемых на накопитель данных для некоторых вычислительных задач. Реализация данной угрозы возможна при условии интенсивного файлового ввода-вывода в кластерной файловой подсистеме суперкомпьютера, основанной на использовании параллельной файловой системы	Внутренний нарушитель с низким потенциалом	Система хранения данных суперкомпьютера	0	0	1
107	Угроза отключения контрольных датчиков	Угроза заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путём прерывания канала связи с контрольными датчиками, следящими за параметрами состояния системы, или нарушения работы самих датчиков. При этом система перестанет реагировать как на инциденты безопасности (если отключённые датчики являлись частью системы безопасности, например, датчики движения), так и на другие типы инцидентов (например, при отключении датчиков пожарной сигнализации, повышения давления в гидроагрегатах и др.). Данная угроза обусловлена слабостями мер защиты информации в автоматизированных системах управления технологическими процессами, а также наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна при условии получения доступа (физического или программного) к линиям связи системы безопасности с контрольными датчиками или к самим датчикам	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	0	1	1
108	Угроза ошибки обновления гипервизора	Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления. Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: – сбоев в процессе его обновления; – обновлений, в ходе которых внедряются новые ошибки в код гипервизора; – обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; – других инцидентов безопасности информации	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, гипервизор	1	1	1
109	Угроза перебора всех настроек и параметров приложения	Угроза заключается в возможности получения нарушителем доступа к дополнительному скрытому функционалу (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличии от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	0	1	1
110	Угроза перегрузки грид-системы вычислительными заданиями	Угроза заключается в возможности снижения пропускной способность ресурсных центров при отправке большого количества заданий одним пользователем (нарушителем) случайно или намеренно, что может сделать невозможной постановку заданий другими пользователями грид-системы в очередь на выполнение. Данная угроза обусловлена слабостями мер по контролю в грид-системе за количеством вычислительных заданий, запускаемых пользователями грид-системы.	Внутренний нарушитель с низким потенциалом	Ресурсные центры грид-системы	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна при условии наличия у нарушителя прав на постановку заданий в очередь на выполнение грид-системой					
111	Угроза передачи данных по скрытым каналам	Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы путём её нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путём её маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография), использования скрытых пикселей («пикселей отслеживания») и т.п. Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при: – наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; – доступа к каналам передачи данных; – посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик	1	0	0
112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Угроза заключается в возможности повреждения нарушителем исполнительных механизмов, заготовки и (или) обрабатывающего инструмента оборудования с числовым программным управлением путём передачи на него команд, приводящих к перемещению обрабатывающего инструмента за допустимые пределы (т.е. команд, запрещённых для оборудования с числовым программным управлением). Данная угроза обусловлена слабостями мер по защите оборудования с числовым программным управлением от выполнения запрещённых команд. Реализация данной угрозы возможна при наличии у нарушителя привилегий на передачу команд на оборудование с числовым программным управлением или возможности изменения команд, передаваемых легальным пользователем	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение	0	1	0
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо) при выполнении следующих условий: – наличие в системе открытых сессий работы пользователей; – наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, аппаратное обеспечение	0	1	1
114	Угроза переполнения целочисленных переменных	Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путём подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определённые типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; – возможности взаимодействия с входным интерфейсом дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств. Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	1	0	0
116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: – наличие у нарушителя доступа к дискредитируемой вычислительную сети; – неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевой трафик	1	0	0
117	Угроза перехвата привилегированного потока	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями (к привилегированному потоку данных), путём синхронного (вызов привилегированной функции, возвращающей неправильное значение) или асинхронного (создание обратных вызовов, манипулирование указателями и т.п.) деструктивного программного воздействия на него. Данная угроза обусловлена уязвимостями программного обеспечения, использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками (наличие ошибочных указателей, некорректное освобождение памяти и т.п.). Реализация данной угрозы возможна в следующих условиях: – в дискредитируемом приложении существуют участки кода, требующие исполнения с правами, превышающими права обычных пользователей; – нарушитель обладает привилегиями, позволяющими вносить изменения во входные данные дискредитируемого приложения	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
118	Угроза перехвата привилегированного процесса	Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов. Реализация данной угрозы возможна при выполнении одного из условий: – успешного введения нарушителем некорректных данных, приводящих к переполнению буфера или к реализации некоторых типов программных инъекций;	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		– наличия у нарушителя привилегий на запуск системных утилит, предназначенных для управления процессами					
119	Угроза перехвата управления гипервизором	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём эксплуатации уязвимостей консоли управления гипервизором. Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, гипервизор, консоль управления гипервизором	1	1	1
120	Угроза перехвата управления средой виртуализации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Информационная система, системное программное обеспечение	1	1	1
121	Угроза повреждения системного реестра	Угроза заключается в возможности нарушения доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр. Данная угроза обусловлена слабостями мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы. Реализация данной угрозы возможна при одном из условий: – возникновения ошибок в работе отдельных процессов или всей операционной системы; – наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы, реестр	0	1	1
122	Угроза повышения привилегий	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации). Реализация данной угрозы возможна при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение, информационная система	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
123	Угроза подбора пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: – нарушитель может осуществить физический доступ к компьютеру и имеет возможность его перезагрузить; – нарушитель обладает специальным программным средством перебора паролей BIOS/UEFI и привилегиями в системе на установку и запуск таких средств	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	0	1
124	Угроза подделки записей журнала регистрации событий	Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: – технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; – технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	0	1	0
125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Угроза заключается в возможности осуществления нарушителем перехвата трафика беспроводной сети или других неправомерных действий путём легализации нарушителем собственного подключения к беспроводной сети в полуавтоматическом режиме (например, WPS) без ввода ключа шифрования. Данная угроза обусловлена слабостями процедуры аутентификации беспроводных устройств в ходе полуавтоматического подключения. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к беспроводной точке доступа, поддерживающей полуавтоматический режим подключения	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	1	1
126	Угроза подмены беспроводного клиента или точки доступа	Угроза заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического подключения точек беспроводного доступа или клиентского программного обеспечения к доверенным субъектам сетевого взаимодействия, подменённым нарушителем. Данная угроза обусловлена слабостями механизма аутентификации субъектов сетевого взаимодействия при беспроводном доступе. Реализация данной угрозы возможна в случае размещения нарушителем клиента или точки беспроводного доступа со специально сформированными параметрами работы (такими как MAC-адрес, название, используемый стандарт передачи данных и т.п.) в зоне доступности для дискредитируемых устройств беспроводного доступа	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка беспроводного доступа	1	0	1
127	Угроза подмены действия пользователя путём обмана	Угроза заключается в возможности нарушителя выполнения неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии (обмана пользователя, навязывание ложных убеждений) или технических методов (использование прозрачных кнопок, подмена надписей на элементах управления и др.) Данная угроза обусловлена слабостями интерфейса взаимодействия с пользователем или ошибками пользователя. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя прав на проведение нужных от него нарушителю операций	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
128	Угроза подмены доверенного пользователя	Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и т.п.	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0	0
129	Угроза подмены резервной копии программного обеспечения BIOS	Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания или создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения BIOS/UEFI, предварительно подменённой нарушителем. Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в следующих условиях: – нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; – возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)	Внутренний нарушитель с низким потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI	0	1	0
130	Угроза подмены содержимого сетевых ресурсов	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения. Реализация данной угрозы возможна при условии наличия у нарушителя прав на доступ к сетевым ресурсам и отсутствии у пользователя сети мер по обеспечению их целостности	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	1	0	0
131	Угроза подмены субъекта сетевого доступа	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	1	1	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения					
132	Угроза получения предварительной информации об объекте защиты	Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и др., путём проведения мероприятий по сбору и анализу доступной информации о системе. Данная угроза обусловлена наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы: – анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию (о трассировке стека, о конфигурации системы, о маршруте прохождения сетевых пакетов) – анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам). – Данная угроза отличается от угрозы перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	1	0	0
133	Угроза получения сведений о владельце беспроводного устройства	Угроза заключается в возможности раскрытия нарушителем сведений о географических перемещениях дискредитируемого пользователя в определённые промежутки времени, в том числе выявить место его работы, проживания и т.п. Получение таких сведений может использоваться нарушителем в дальнейшем для реализации угроз в информационных системах, доступ к которым имеет дискредитируемый пользователь. Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет. Реализация данной угрозы возможна при условии наличия у нарушителя доступа к идентификационными данным стационарных точек беспроводного доступа, с которыми в автоматическом режиме осуществляет взаимодействие беспроводное устройство дискредитируемого пользователя	Внешний нарушитель с низким потенциалом	Сетевой узел, метаданные	1	0	0
134	Угроза потери доверия к поставщику облачных услуг	Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невосполнимого оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику. Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок. Реализация данной угрозы возможна в случае обнародования единичных или множественных фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, повлёкших значительные убытки для его клиентов	Внутренний нарушитель со средним потенциалом	Объекты файловой системы, информационная система, иммигрированная в облако	1	1	1
135	Угроза потери и утечки данных, обрабатываемых в облаке	Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе. Данная угроза обусловлена слабостями мер защиты информации, обрабатываемой в облачной системе.	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, метаданные,	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна в случае допущения поставщиком (некорректный выбор или настройка средств защиты) или потребителем (потеря пароля, электронного ключа, вход с небезопасной консоли) облачных услуг ошибок при обеспечении безопасности защищаемой информации		объекты файловой системы			
136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Угроза заключается в возможности допуска ошибок при копировании защищаемой информации при распределённом хранении данных на различных узлах хранилища больших данных вследствие несогласованности их работы, влекущих за собой невозможность осуществления легальным пользователем доступа к блокам или ко всей защищаемой информации. Данная угроза обусловлена слабостями механизмов репликации данных, реализованных в узлах хранилища больших данных. Реализация данной угрозы возможна в условиях отключения или выведения из строя одного или нескольких узлов за счёт специальных программных воздействий на узлы хранилища больших данных, а также возникновения технических или программных сбоев в работе их компонентов	Внутренний нарушитель с низким потенциалом	Информационная система, узлы хранилища больших данных	0	1	1
137	Угроза потери управления облачными ресурсами	Угроза заключается в возможности нарушения договорных обязательств со стороны поставщика облачных услуг в отношении их потребителя из-за значительной сложности построения эффективной системы управления облачными ресурсами облачной системы, особенно использующей облачные ресурсы других поставщиков облачных услуг. Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг. Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется (или становится невозможным) из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика	Внешний нарушитель с высоким потенциалом	Сетевой трафик, объекты файловой системы	1	1	1
138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Угроза заключается в возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако, со стороны поставщика облачных услуг из-за отсутствия у него сведений об особенностях управления конкретной системы, а также из-за отсутствия у потребителя облачных услуг, обладающего такими сведениями, возможности проводить весь комплекс работ по управлению инфраструктурой собственной системы в связи с её иммиграцией в облако. Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации. Реализация данной угрозы возможна в случаях передачи поставщику облачных услуг части функций управления системой потребителя облачных услуг (при миграции части или всей системы в облако)	Внутренний нарушитель со средним потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	1	1	1
139	Угроза преодоления физической защиты	Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)	Внешний нарушитель со средним потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	1	1	1
140	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким	Информационная система, сетевой узел, системное	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена тем, что для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы	потенциалом	программное обеспечение, сетевое программное обеспечение, сетевой трафик			
141	Угроза привязки к поставщику облачных услуг	Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)	Внутренний нарушитель с низким потенциалом	Информационная система, иммигрированная в облако, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, объекты файловой системы	0	0	1
142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Угроза заключается в возможности снижения качества облачных услуг (или даже отказа в их оказании конечным потребителям) из-за возникновения технических сбоев хотя бы у одного из поставщиков облачных услуг (входящих в цепь посредников при оказании облачных услуг их конечному потребителю), а также из-за возникновения существенных задержек или потерь в каналах передачи данных, арендуемых потребителем или поставщиками облачных услуг. Данная угроза обусловлена слабостями процедуры контроля за выполнением технического обслуживания и соблюдением режимов функционирования технических средств облачной информационной системы. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы		Системное программное обеспечение, аппаратное обеспечение, канал связи	0	0	1
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	0	0	1
144	Угроза программного сброса пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера путём ввода «пустого» пароля. Данная угроза обусловлена слабостями мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI.	Внутренний нарушитель с низким потенциалом	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	1	1	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Реализация данной угрозы возможна при условиях: – наличия в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля непосредственно из-под операционной системы; – наличия у нарушителя специальных программных средств, реализующих сброс пароля, а также прав в операционной системе для установки и запуска данных средств					
145	Угроза пропуска проверки целостности программного обеспечения	Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения. Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов: «ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	0	1	1
146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Угроза заключается в возможности осуществления процессом нарушителя, функционирующем в вычислительном поле суперкомпьютера, считывания защищаемых данных из оперативной памяти, выделенной для параллельного (дискредитируемого) процесса, с использованием операций удалённого прямого доступа к памяти. Данная угроза обусловлена слабостями протокола прямого доступа к оперативной памяти, с помощью которого выполняется обращение к сегменту памяти, выделенному для удалённого параллельного процесса, функционирующего в вычислительном поле суперкомпьютера. Реализация данной угрозы возможна при условии успешного осуществления нарушителем доступа к входным/выходным данным параллельных процессов в вычислительном поле суперкомпьютера	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Вычислительные узлы суперкомпьютера, каналы передачи данных суперкомпьютера, системное программное обеспечение	1	0	0
147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Угроза заключается в возможности автоматического распространения на всю грид-систему несанкционированно полученных нарушителем на одном узле привилегий. Данная угроза обусловлена наличием уязвимостей в клиентском программном обеспечении грид-системы и слабостями в механизме назначения прав пользователям, реализованном в связующем программном обеспечении. Реализация данной угрозы возможна при условии успешного повышения нарушителем своих прав на одном узле грид-системы	Внутренний нарушитель со средним потенциалом	Ресурсные центры грид-системы, узлы грид-системы, грид-система, сетевое программное обеспечение	1	1	0
148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Угроза заключается в возможности возникновения ситуаций, связанных с ошибками автоматического назначения пользователям прав доступа (наделение дополнительными полномочиями, ошибочное наследование, случайное восстановление «неактивных» учётных записей т.п.). Данная угроза обусловлена слабостями мер контроля за большим количеством (от тысячи, а в некоторых случаях и до нескольких миллионов) учётных записей пользователей со стороны администраторов безопасности. Реализация данной угрозы возможна при условии возникновения сбоев или ошибок в работе системы разграничения доступа хранилища больших данных		Информационная система, система разграничения доступа хранилища больших данных	1	0	1
149	Угроза сбоя обработки специальным образом изменённых файлов	Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путём вызова сбоя в их работе за счёт внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Метаданные, объекты файловой системы, системное	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных. Реализация данной угрозы возможна в условиях: – наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке; – успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя		программное обеспечение			
150	Угроза сбоя процесса обновления BIOS	Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение BIOS/UEFI в результате нарушения процесса его обновления. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке повреждённой/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и совместимости)	Внутренний нарушитель со средним потенциалом	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	0	0	1
151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Угроза заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера. Данная угроза обусловлена недостаточностью мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям. Реализация данной угрозы возможна при наличии у нарушителя сетевого доступа к исследуемому сетевому ресурсу и специальных программных средств сканирования сети	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение, сетевой узел	1	0	0
152	Угроза удаления аутентификационной информации	Угроза заключается в возможности отказа легитимным пользователям в доступе к информационным ресурсам, а также в возможности получения нарушителем привилегий дискредитированного пользователя за счёт сброса (обнуления, удаления) его аутентификационной информации. Данная угроза обусловлена слабостями политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями пользователей. Реализация данной угрозы возможна при выполнении одного из следующих условий: – штатные средства работы с учётными записями пользователей обладают функционалом сброса аутентификационной информации, и нарушитель получил привилегии в дискредитируемой системе на использование данных средств; – нарушитель обладает специальным программным обеспечением, реализующим функцию сброса аутентификационной информации, и получил привилегии в дискредитируемой системе на использование данных средств	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	1	1	1
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объёмом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объём сетевых запросов, формируемых нарушителем. Данная угроза обусловлена слабостями мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов; – сведений о сетевом адресе дискредитируемой системы; – специального программного обеспечения, реализующего функции генерации сетевых пакетов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Микропрограммное обеспечение BIOS/UEFI	1	1	1
155	Угроза утраты вычислительных ресурсов	Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за исчерпания нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов». Данная угроза обусловлена слабостями механизма контроля за распределением вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы; – привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе; – отсутствие у администраторов возможности: для техники «утечки ресурсов» – перезагрузки системы во время отправки нарушителем большого числа запросов на выделение ресурсов, а для техники «выделения ресурсов» – форсированного освобождения ресурсов, выделенных по запросам вредоносных процессов	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	0	0	1
156	Угроза утраты носителей информации	Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников	Внутренний нарушитель с низким потенциалом	Носитель информации	1	0	1
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	0	1	1
158	Угроза форматирования носителей информации	Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации. Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: – время, прошедшее после форматирования; – тип носителя информации; – тип файловой системы носителя; – интенсивность взаимодействия с носителем после форматирования и др.	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Носитель информации	0	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
159	Угроза «форсированного веб-браузинга»	Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	0	0
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)	Внешний нарушитель с низким потенциалом	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	1	0	1
161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля суперкомпьютера. Данная угроза обусловлена слабостями мер контроля за распределением вычислительных ресурсов суперкомпьютера при обработке задачи несколькими процессорами. Реализация данной угрозы возможна при условии выполнения суперкомпьютером специфичных вычислительных задач, в ходе которых генерируются межпроцессорные сообщения с большой интенсивностью	Внутренний нарушитель с низким потенциалом	Вычислительные узлы суперкомпьютера	0	0	1
162	Угроза эксплуатации цифровой подписи программного кода	Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: – дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; – дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); – нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение	1	1	1
163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путём перехвата исключений/сигналов, сгенерированных участком программного кода, исполняемого с повышенными привилегиями (привилегированным блоком функций) и содержащего команды по управлению защищаемой информацией. Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения доступа. Реализация данной угрозы возможна при следующих условиях: – дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java); – в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока); – нарушитель обладает правами, достаточными для перехвата программных исключений в системе	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Системное программное обеспечение	1	1	1
164	Угроза распространения состояния «отказ в	Угроза заключается в возможности распространения негативных последствий от реализации угроз на физическом или виртуальном уровне облачной инфраструктуры на уровни	Внешний нарушитель с низким потенциалом, Внутренний	Облачная инфраструктура, созданная с	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
	обслуживании» в облачной инфраструктуре	управления и оркестровки, а также на все информационные системы, развёрнутые на базе дискредитированной облачной инфраструктуры. Данная угроза обусловлена невозможностью функционирования информационных систем в облаке при некорректной работе самой облачной инфраструктуры, а также зависимостью работоспособности верхних уровней облачной инфраструктуры от работоспособности нижних. Реализация данной угрозы возможна в случае приведения облачной инфраструктуры на физическом или виртуальном уровне облачной инфраструктуры в состояние «отказ в обслуживании»	нарушитель с низким потенциалом	использованием технологий виртуализации			
165	Угроза включения в проект не достоверно испытанных компонентов	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированности и др.	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	1	1	1
166	Угроза внедрения системной избыточности	Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) из-за внедрения в него (в неё) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой)	Внутренний нарушитель со средним потенциалом	Программное обеспечение, информационная система, ключевая система информационной инфраструктуры	0	0	1
167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым	Внутренний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	1	1	1
168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём получения информации идентификации/аутентификации, соответствующей учётной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условиях: – наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учётная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего, его отключили); – наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	0	1
169	Угроза наличия механизмов разработчика	Угроза заключается в возможности перехвата управления программой за счёт использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки).	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации. Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы					
170	Угроза неправомерного шифрования информации	Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов	Внешний нарушитель с низким потенциалом	Объект файловой системы	0	0	1
171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств и др.), подключённых к сети Интернет, за счёт захвата управления такими устройствам путём несанкционированной установки на них: вредоносного ПО типа Backdoor для обеспечения нарушителя возможностью удалённого доступа/управления дискредитируемым вычислительным устройством; клиентского ПО для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа «отказ в обслуживании» и др.). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевое программное обеспечение	0	0	1
172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	1	1	1
173	Угроза «спама» веб-сервера	Угроза заключается в возможности неправомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов. Данная угроза обусловлена уязвимостями механизмов фильтрации сообщений, поступающих из сети Интернет. Реализация данной угрозы возможна при условии наличия в дискредитируемом веб-сервере активированного функционала, реализующего различные почтовые сервера, службы доставки мгновенных сообщений, блоги, форумы, аукционы веб-магазинов, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.	Внешний нарушитель с низким потенциалом	Сетевое программное обеспечение	0	0	1
174	Угроза «фарминга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём скрытного перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; – средств создания и запуска поддельного сайта;	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		– специальных программных средств типа «эксплойт», реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа					
175	Угроза «фишинга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме. Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга». Реализация данной угрозы возможна при условии наличия у нарушителя: – сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; – средств создания и запуска поддельного сайта; – сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик	1	0	0
176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз ИБ. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации	Внешний нарушитель с низким потенциалом	Средство защиты информации	0	0	1
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). Реализуемость данной угрозы зависит от требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью, а также разницей между этими требованиями и фактическим уровнем обнаружения и исправления ошибок	Внутренний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	0	1	1
178	Угроза несанкционированного использования системных и сетевых утилит	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счёт использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях:	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Системное программное обеспечение	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		– наличие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему и сокрытие (с использованием существующих архивов, атрибутов «скрытый» или «только для чтения» и др.); – наличие у нарушителя привилегий на запуск таких утилит					
179	Угроза несанкционированной модификации защищаемой информации	Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём. Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Объекты файловой системы	0	1	0
180	Угроза отказа подсистемы обеспечения температурного режима	Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима	Внешний нарушитель со средним потенциалом, Внутренний нарушитель с низким потенциалом	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД, программируемые логические контроллеры, распределённые системы контроля, управленческие системы и другие программные средства контроля	0	0	1
181	Угроза перехвата одноразовых паролей в режиме реального времени	Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путём перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечёт их срок действия (обычно, не более 5 минут). Реализация данной угрозы возможна при выполнении следующих условий: – наличие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия; – успешное осуществление нарушителем перехвата трафика между системой и пользователем	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	0	1	0
182	Угроза физического устаревания аппаратных компонентов	Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем	Внутренний нарушитель с низким потенциалом	Аппаратное средство	0	0	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных. Данная угроза обусловлена наличием у автоматизированной системы управления технологическими процессами программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к: – блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия; – нарушению штатного хода технологических процессов; – частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя; – аварийной ситуации в критической системе информационной инфраструктуры	Внешний нарушитель с высоким потенциалом, Внутренний нарушитель со средним потенциалом	Программное обеспечение автоматизированной системы управления технологическими процессами	0	1	1
184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: – персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); – информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); – данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); – видеоданные, снимаемые видеокамерами мобильного устройства; – аудиоданные, снимаемые микрофоном устройства	Внутренний нарушитель со средним потенциалом	Мобильное устройство	1	0	0
185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки средства защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к конфигурационным файлам средства защиты информации. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Средство защиты информации	1	1	1
186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов в сети Интернет	Внутренний нарушитель с низким потенциалом	Сетевое программное обеспечение	0	1	1
187	Угроза несанкционированного воздействия на средство защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования.	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним	Средство защиты информации	1	1	1

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		Угроза обусловлена наличием у средств защиты информации программной среды управления и взаимодействия с пользователями системы. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации	потенциалом				
188	Угроза подмены программного обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети Интернет. Реализация данной угрозы возможна при скачивании программного обеспечения в сети Интернет	Внутренний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	1	1	1
189	Угроза маскирования действий вредоносного кода	Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации. Реализация данной угрозы возможна при условии использования в системе устаревших версий средств защиты информации	Внешний нарушитель со средним потенциалом	Системное программное обеспечение, сетевое программное обеспечение	0	1	1
190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: – неограниченном доступе пользователя в сеть Интернет; – наличии у нарушителя сведений о сайтах, посещаемых пользователем	Внешний нарушитель со средним потенциалом	Сетевое программное обеспечение	1	1	1
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	1	1	1
192	Угроза использования уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	1	1	1
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная у гроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов. Реализация данной угрозы возможна:	Внешний нарушитель со средним потенциалом	Информационные ресурсы, объекты файловой системы	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
		– при условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения; – при отсутствии или недостаточной реализации мер межсетевого экранирования					
194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Угроза заключается в возможности снятия нарушителем предустановленных производителем ограничений на конфигурирование привилегированных функций мобильного устройства. Данная угроза обусловлена наличием уязвимостей в операционных системах мобильного устройства, позволяющих получить доступ к настройкам привилегированных функций. Реализация данной угрозы возможна при получении нарушителем доступа к мобильному устройству	Внешний нарушитель с высоким потенциалом	Мобильное устройство	1	1	1
195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Угроза заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему. Данная угроза обусловлена ошибками в процессорах (например, ошибками в процессоре Intel поколения Haswell), позволяющими за счет создания специальных приложений осуществлять обход механизмов защиты, встроенных в операционную систему (например, механизма ASLR). Реализация данной угрозы возможна при: – инициировании коллизии в таблице целевых буферов - с ее помощью можно узнать участки памяти, где находятся конкретные фрагменты кода; – создании приложения, использующего эти фрагменты кода для обхода механизма защиты; – запуске данного приложения в связке с эксплойтом какой-либо уязвимости самой операционной системы для создания возможности удаленного запуска вредоносного кода	Внешний нарушитель с высоким потенциалом	Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)	0	1	0
196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем	Внешний нарушитель с высоким потенциалом	Мобильное устройство (аппаратное устройство)	0	1	1
197	Угроза хищения аутентификационной информации из временных файлов cookie	Угроза заключается в возможности хищения с использованием вредоносной программы аутентификационной информации пользователей, их счетов, хранящейся во временных файлах cookie, и передачи этой информации нарушителям через открытый RDP-порт. Данная угроза обусловлена недостаточностью мер антивирусной защиты, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена непринятием мер по стиранию остаточной информации из временных файлов (очистке временных файлов). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	Внешний нарушитель со средним потенциалом	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	1	0	0
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	Внешний нарушитель со средним потенциалом	Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)	0	1	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Мобильное устройство и запущенные на нем приложения (программное обеспечение, аппаратное устройство)	1	0	1
200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Угроза заключается в возможности хищения данных пользователя с его мобильного устройства через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающейся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть не отключен) и установлена низкая чувствительность голосового идентификатора	Внешний нарушитель со средним потенциалом	Данные пользователя мобильного устройства (аппаратное устройство)	1	0	0
201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации. Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации. Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации	Внешний нарушитель со средним потенциалом	Аутентификационные данные пользователя (программное обеспечение)	1	0	0
202	Угроза несанкционированной установки приложений на мобильные устройства	Угроза заключается в возможности установки приложений на виртуальные машины мобильных устройств, работающих под управлением операционной системы Android, несанкционированно запущенных внедренной вредоносной программой. Вредоносная программа запускает виртуальную машину на мобильном устройстве, размещает (устанавливает) в этой виртуальной машине неограниченное количество приложений. Данная угроза обусловлена недостаточностью мер по контролю за запуском прикладного программного обеспечения, что позволяет выполнить неконтролируемый запуск вредоносного прикладного программного обеспечения по факту совершения пользователем различных действий в системе (например, при попытке закрытия пользователем нежелательной рекламы). Реализация данной угрозы возможна при условии наличия на мобильном устройстве вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение	Внешний нарушитель со средним потенциалом	Мобильные устройства (аппаратное устройство, программное обеспечение)	1	0	0
203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Угроза заключается в возможности хищения данных с неподключенных к сети Интернет компьютеров за счет компрометации их аппаратных элементов или устройств коммутационного оборудования (например, маршрутизаторов), оснащенных LED-индикаторами, фиксации мерцания этих индикаторов и расшифровки полученных результатов. Реализация данной угрозы обусловлена тем, что существует возможность несанкционированного получения управления этими индикаторами (с помощью специальной прошивки или повышения привилегий и выполнения вредоносного кода), позволяющего передавать информацию путем ее преобразования в последовательность сигналов индикаторов компьютеров и коммутационного оборудования. Реализация данной угрозы возможна при условии, что злоумышленником получен физический доступ к компрометируемому компьютеру или коммутационному оборудованию для установки средства визуального съема сигналов LED-индикаторов	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Программное обеспечение	1	0	0

ID угрозы	Наименование угрозы	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиден-циальности	Нарушение целостности	Нарушение доступности
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах. Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации. Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет	Внешний нарушитель со средним потенциалом	Аппаратное устройство	0	1	0
205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Угроза заключается в возможности нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов. Реализация данной угрозы обусловлена тем, что на компьютере установлено средство защиты информации, реализующее функцию блокирования файлов	Внешний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение	0	0	1
206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Угроза заключается в прекращении работы оборудования с ЧПУ, вызванном изменением геолокационной информации о данном оборудовании. Угроза обусловлена геолокационной привязкой оборудования с ЧПУ к конкретной географической координате при пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации	Внешний нарушитель с высоким потенциалом	Аппаратное устройство	1	0	1
207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Угроза заключается в несанкционированном получении доступа к параметрам настройки информации в оборудовании с ЧПУ посредством использования специальных «мастер-кодов» (инженерных паролей), «жестко прописанных» (не изменяемых путем конфигурирования) в программном обеспечении данного оборудования. Угроза обусловлена необходимостью проведения ремонтных работ при сбоях в ПО оборудования с ЧПУ представителями производителя	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Аппаратное устройство, программное обеспечение	1	1	1

Определение потенциала нарушителя, необходимого для реализации угрозы ИБ

Настоящее приложение применяется для определения потенциала, необходимого для реализации угрозы ИБ, данные по которой отсутствуют в банке данных угроз ИБ, и характеристики которых определяются на основе иных источников или результатов исследований.

Приведенный подход к оценке потенциала нарушителя направлен на снижение уровня субъективности и неопределенности при оценке потенциала нарушителя, который требуется для реализации угрозы ИБ в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

Исходными данными для определения потенциала нарушителя являются: данные об аппаратном, общесистемном и прикладном программном обеспечении, применяемых информационных технологиях, особенностях функционирования информационной системы;

данные об уязвимостях в аппаратном, общесистемном и прикладном программном обеспечении, опубликованные в различных базах данных уязвимостей, полученные в результате исследований (тестировании) или полученные от уполномоченных федеральных органов исполнительной власти и организаций.

При оценке потенциала нарушителя необходимо исходить из того, что для успешного достижения целей реализации угроз ИБ, нарушителю необходимо осуществить подготовку к реализации угрозы и непосредственно реализацию угрозы ИБ. При этом не единственным, но необходимым условием на этапе подготовки к реализации угрозы ИБ является идентификация уязвимостей в информационной системе, а на этапе реализации угрозы ИБ – использование уязвимостей информационной системы.

Таким образом, для определения потенциала нарушителя необходимо оценить возможности нарушителя идентифицировать уязвимости и использовать их в информационной системе в ходе подготовки к реализации и непосредственно в ходе реализации угрозы ИБ. Для проведения указанной оценки делается предположение о наличии уязвимостей, которые потенциально содержатся в информационной системе и могут быть использованы для реализации угрозы ИБ.

Потенциальные уязвимости определяются для каждого класса и типа программного обеспечения и для каждого узла (хоста) информационной системы исходя из условия, что для реализации угрозы ИБ нарушителю необходимо идентифицировать и использовать как минимум одну уязвимость на каждом узле и хосте.

В качестве исходных данных для определения потенциальных уязвимостей используются данные по составу информационной системы и особенностям ее функционирования, а также данные об уязвимостях в этом программном обеспечении, опубликованные в общедоступных источниках, полученные по результатам исследований и (или) полученные от уполномоченных органов и организаций.

Для каждой выявленной потенциальной уязвимости проводится оценка возможностей ее идентификации и использования в информационной системе нарушителем, обладающим определенными возможностями и для каждого из возможных сценариев реализации угрозы ИБ.

Оценка возможностей нарушителя по идентификации и использованию уязвимости в информационной системе проводится по результатам определения следующих показателей:

- время, затрачиваемое нарушителем на идентификацию и использование уязвимости (затрачиваемое время);
- техническая компетентность нарушителя;
- знание нарушителем проекта и информационной системы; оснащенность нарушителя;
- возможности нарушителя по доступу к информационной системе.

Во многих случаях указанные показатели являются зависимыми и могут в различной степени заменять друг друга. В частности, показатели технической компетентности или оснащенности могут заменяться показателем затрачиваемого времени.

Определение показателя «затрачиваемое время»

Показатель «затрачиваемое время» характеризует время, непрерывно затрачиваемое нарушителем для идентификации и использования уязвимости для реализации угрозы ИБ.

Показатель «затрачиваемое время» может принимать значения «за минуты», «за часы», «за дни» или «за месяцы».

Значение «за минуты» присваивается, если для реализации угрозы ИБ нарушитель затратит менее получаса на идентификацию и использование уязвимости.

Значение «за часы» присваивается, если для реализации угрозы ИБ нарушитель затратит менее чем один день на идентификацию и использование уязвимости.

Значение «за дни» присваивается, если для реализации угрозы ИБ нарушитель затратит менее чем один месяц на идентификацию и использование уязвимости.

Значение «за месяцы» присваивается, если для реализации угрозы ИБ нарушитель затратит, как минимум, месяц на идентификацию и использование уязвимости.

Определение показателя «техническая компетентность нарушителя»

Показатель «техническая компетентность нарушителя» характеризует, каким уровнем знаний и подготовкой в области информационных технологий и защиты информации должен обладать нарушитель, чтобы идентифицировать и использовать уязвимости для реализации угрозы ИБ.

Показатель «техническая компетентность нарушителя» может принимать значения «специалист», «профессионал» или «непрофессионал».

Значение «профессионал» присваивается, если нарушитель имеет хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе, а также обладает специальными знаниями о методах и средствах выявления новых уязвимостей и способах реализации угроз ИБ для информационных систем данного типа.

Значение «специалист» присваивается, если нарушитель имеет осведомленность о мерах защиты информации, применяемых в информационной системе данного типа.

Значение «непрофессионал» присваивается, если нарушитель имеет слабую осведомленность (по сравнению со специалистами или профессионалами) о мерах защиты информации, применяемых в информационных системах данного типа, и не обладает специальными знаниями по реализации угроз ИБ.

Определение показателя «знание нарушителем проекта и информационной системы»

Показатель «знание нарушителем проекта и информационной системы» характеризует, какие сведения об информационной системе и условиях ее эксплуатации доступны нарушителю, чтобы идентифицировать и использовать уязвимости для реализации угрозы ИБ.

Показатель «знание нарушителем проекта и информационной системы» может принимать значения «отсутствие знаний», «ограниченные знания» или

«знание чувствительной информации».

Значение «отсутствие знаний» присваивается, если в результате принятия мер по защите информации нарушителю не может стать известно о структурно-функциональных характеристиках информационной системы, системе защиты информации информационной системы, а также об иной информации по разработке (проектированию) и эксплуатации информационной системы, включая сведения из конструкторской, проектной и эксплуатационной документации. При этом может быть доступна информация о целях и задачах, решаемых информационной системой. Данный показатель также присваивается, если сведения об информационной системе отнесены к информации ограниченного доступа и не могут быть доступны для неограниченного круга лиц.

Значение «ограниченные знания» присваивается, если нарушителю наряду с информацией о целях и задачах, решаемых информационной системой, может стать известна только эксплуатационная документация на информационную систему (в частности руководство пользователя и (или) правила эксплуатации информационной системы).

Значение «знание чувствительной информации» присваивается, если нарушителю может стать известны конструкторская (проектная) и эксплуатационная документация на информационную систему, информация о структурно-функциональных характеристиках информационной системы, системе защиты информационной системы.

г) определение показателя «возможности нарушителя по доступу к информационной системе»

Показатель «возможности нарушителя по доступу к информационной системе» характеризует, как долго по времени нарушитель должен иметь возможность доступа к информационной системе для идентификации и использования уязвимостей для реализации угроз ИБ.

Показатель «возможности нарушителя по доступу к информационной системе» может принимать значения «за минуты», «за часы», «за дни» или «за месяцы».

Значение «за минуты» присваивается, если для идентификации и использования уязвимости для реализации угрозы ИБ нарушителю требуется доступ менее получаса.

Значение «за часы» присваивается, если для идентификации и использования уязвимости для реализации угрозы ИБ нарушителю требуется доступ менее одного дня.

Значение «за дни» присваивается, если для идентификации и использования уязвимости для реализации угрозы ИБ нарушителю требуется доступ менее одного месяца.

Значение «за месяцы» присваивается, если для идентификации и использования уязвимости для реализации угрозы ИБ нарушителю требуется доступ более одного месяца.

Показатель «возможности нарушителя по доступу к информационной системе» взаимосвязан с показателем «затраченное время». Идентификация и использование уязвимости при реализации угрозы ИБ могут требовать продолжительного времени по доступу к информационной системе, что увеличивает возможность обнаружения уязвимости. В отдельных случаях продолжительный доступ к информационной системе не требуется (методы и средства реализации угроз безопасности разрабатываются автономно), но при этом требуется кратковременный доступ к информационной системе.

определение показателя «оснащенность нарушителя»

Показатель «оснащенность нарушителя» характеризует, какие программные и (или) программно-технические средства требуются нарушителю для идентификации и использования уязвимостей для реализации угроз ИБ.

Показатель «оснащенностьнарушителя» может принимать значения «стандартное оборудование», «специализированное оборудование» или «оборудование, сделанное на заказ».

Значение «стандартное оборудование» присваивается, если для идентификации или использования уязвимостей при реализации угрозы ИБ требуются программные (программно-технические) средства, легко доступные для нарушителя. К таким средствам, в первую очередь, относятся программные средства непосредственно информационной системы (отладчик в операционной системе, средства разработки и иные), программные средства, которые могут быть легко получены (программы, имеющиеся в свободном доступе в сети Интернет) или имеются простые сценарии реализации угроз.

Значение «специализированное оборудование» присваивается, если для идентификации или использования уязвимостей при реализации угрозы ИБ требуются программные (программно-технические) средства, которые отсутствуют в свободном доступе, но могут быть приобретены нарушителем без значительных усилий. К таким средствам, в первую очередь, относятся программные (программно-технические) средства, которые имеются в продаже (анализаторы кода, анализаторы протоколов и иные) или требуется разработка более сложных программ и сценариев реализации угрозы. Оборудование может быть закуплено, либо, например, могут быть использованы компьютеры, объединенные через сеть Интернет (бот-сети).

Значение «оборудование, сделанное на заказ» присваивается, если для идентификации или использования уязвимостей при реализации угрозы ИБ требуются программные (программно-технические) средства, которые недоступны широкому кругу лиц, так как требуется их специальная разработка с привлечением исследовательских организаций, или распространение этих средств контролируется в соответствии с законодательством. К такому оборудованию также относится дорогостоящие средства или средства, сведения о которых относятся к информации ограниченного доступа.

С целью вычисления потенциала нарушителя определяются числовые значения указанных показателей в соответствии с таблицей 9.

Таблица 9 - Показатели возможностей нарушителя

Показатель возможностей нарушителя		Значения при идентификации уязвимости	Значения при использовании уязвимости
Затрачиваемое время	< 0,5 час	0	0
	< 1 день	2	3

Показатель возможностей нарушителя		Значения при идентификации уязвимости	Значения при использовании уязвимости
	< 1 месяц	3	5
	> 1 месяц	5	8
Техническая компетентность нарушителя	Непрофессионал	0	0
	Специалист	2	3
	Профессионал	5	4
Знание проекта и информационной системы	Отсутствие знаний	0	0
	Ограниченные знания	2	2
	Знание чувствительной информации	5	4
Возможность доступа к информационной системе	< 0,5 час или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не возможно		
Оснащенность нарушителя	Отсутствует	0	0
	Стандартное оборудование	1	2
	Специализированное оборудование	3	4
	Оборудование, сделанное на заказ	5	6

Для конкретной потенциальной уязвимости может возникнуть необходимость определять показатели несколько раз для различных способов реализации угроз ИБ (попеременно использовать разные значения показателей компетентности в сочетании со значениями времени и оборудования). При этом следует выбирать наибольшее значение, полученное при каждом расчете показателей.

Полученные на основе таблицы 9 значения характеристик потенциала нарушителя суммируются. Полученная сумма значений характеристик соотносится с диапазонами значений, приведенных в таблице 10, в соответствии с которой определяется потенциал нарушителя, необходимый для реализации угрозы ИБ.

Таблица 10 - Необходимый потенциал нарушителя

Диапазон значений	Потенциал нарушителя
<10	Потенциал недостаточен для реализации угрозы ИБ
10-17	Базовый (низкий)
18-24	Базовый повышенный (средний)
>24	Высокий

Приложение № 3 к Регламенту

Структура модели угроз ИБ

Модель угроз ИБ содержит следующие разделы:

1. Общие положения.

Описание информационной системы и особенностей ее функционирования

1.1. Цель и задачи, решаемые Активом.

Описание структурно-функциональных характеристик Актива.

1.2. Описание технологии обработки информации.

2. Возможности нарушителей (модель нарушителя).

2.1. Типы и виды нарушителей.

2.2. Возможные цели и потенциал нарушителей.

2.3. Возможные способы реализации угроз ИБ.

3. Определение угроз безопасности информации

3.1. Оценка применимости угроз безопасности информации.

3.2. Оценка вероятности реализации угроз безопасности информации

3.3. Актуальные угрозы ИБ. Приложения (при необходимости).

Раздел «Общие положения» содержит назначение и область действия документа, информацию о полном наименовании информационной системы, для которой разработана модель угроз ИБ, а также информацию об использованных для разработки модели угроз ИБ нормативных и методических документах, национальных стандартах. В данный раздел также включается информация об используемых данных и источниках, на основе которых определяются угрозы ИБ (документация, исходные тексты программ, опросы персонала, журналы регистрации средств защиты, отчеты об аудите и иные источники).

Раздел «Описание информационной системы и особенностей ее функционирования» содержит общую характеристику информационной системы, описание структурно-функциональных характеристик информационной системы, описание взаимосвязей между сегментами информационной системы, описание взаимосвязей с другими информационными системами и информационно-телекоммуникационными сетями, описание технологии обработки информации. Также в данном разделе приводятся предположения, касающиеся информационной системы и особенностей ее функционирования (в частности предположения об отсутствии неучтенных беспроводных каналов доступа или динамичность выделения адресов узлам информационной системы, иные предположения). В раздел включаются любые ограничения, касающиеся информационной системы и особенностей ее функционирования.

Раздел «Возможности нарушителей (модель нарушителя)» содержит описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в Активе, способов реализации угроз ИБ. В данный раздел также включаются предположения, касающиеся нарушителей (в частности предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). В раздел включаются любые ограничения, касающиеся определения нарушителей (в частности исключение администраторов информационной системы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).

Раздел «Определение угроз безопасности информации» содержит описание актуальных угроз безопасности, включающее наименование угрозы ИБ, возможности нарушителя по реализации угрозы, используемые уязвимости информационной системы, описание способов реализации угрозы ИБ, объекты воздействия, возможные результат и последствия от реализации угрозы ИБ.