

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 31 Г. ЙОШКАР-ОЛЫ»**

УТВЕРЖДАЮ

Директор МБОУ «Средняя общеобразовательная  
школа № 31 г. Йошкар-Олы»



*[Handwritten signature]*  
Е.П. Николаев

« 09 » 12 2020 г.

*Приказ от 09.12.2020 № 243*

**ИНФОРМАЦИОННАЯ СИСТЕМА «ОБРАЗОВАНИЕ»  
(ИС «Образование»)**

**МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ  
ДАННЫХ**

г. Йошкар-Ола  
2020

## 1. СОКРАЩЕНИЯ

В настоящем документе применяются следующие обозначения и сокращения:

АС	- автоматизированная система;
АРМ	- автоматизированное рабочее место;
ИСПДн	- информационная система персональных данных;
КЗ	- контролируемая зона;
НДВ	- недокументированные (недекларированные) возможности
НСД	- несанкционированный доступ, несанкционированные действия;
ОС	- операционная система;
ПДн	- персональные данные;
ПК	- программный комплекс;
ПО	- программное обеспечение;
ПЭМИН	- побочные электромагнитные излучения и наводки;
СВТ	- средства вычислительной техники;
СЗИ	- средство защиты информации;
СКЗИ	- средства криптографической защиты информации;
СФ	- среда функционирования СКЗИ;
ТКУИ	- технический канал утечки информации.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**2.1. Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**2.2. Автоматизированное рабочее место** – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

**2.3. Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**2.4. Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**2.5. Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**2.6. Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**2.7. Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**2.8. Доступ к информации** – возможность получения информации и ее использования.

**2.9. Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**2.10. Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**2.11. Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**2.12. Информация** – сведения (сообщения, данные) независимо от формы их представления.

**2.13. Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**2.14. Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**2.15. Контролируемая зона** – пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

**2.16. Модель нарушителя** – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

**2.17. Модель угроз** – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

**2.18. Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**2.19. Недокументированные (недекларированные) возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**2.20. Несанкционированный доступ, несанкционированные действия** – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

**2.21. Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**2.22. Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**2.23. Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**2.24. Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

**2.25. Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**2.26. Операционная система** – совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг.

**2.27. Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**2.28. Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**2.29. Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**2.30. Пользователь** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**2.31. Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**2.32. Программная закладка** – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

**2.33. Программное обеспечение** – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

**2.34. Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**2.35. Ресурс информационной системы персональных данных** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы персональных данных .

**2.36. Среда функционирования СКЗИ** – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

**2.37. Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ)** – средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

**2.38. Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**2.39. Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**2.40. Субъект доступа** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**2.41. Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**2.42. Угроза безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

**2.43. Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**2.44. Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**2.45. Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**2.46. Уязвимость** – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

**2.47. Целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

**2.48. Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

### 3. НОРМАТИВНЫЕ ССЫЛКИ

Система должна соответствовать требованиям следующих Федеральных законов и принятых в соответствии с ними нормативно-правовых актов:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Также при формировании настоящей Модели угроз безопасности ПДн использовались следующие нормативно-правовые документы:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.;
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432;
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения», утвержденный постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399;

– ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст;

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст;

– ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 10 сентября 2014 г. № 1046-ст;

– ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 457-ст;

– ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27 августа 1990 г. № 2467;

– ГОСТ 15971-90 «Системы обработки информации. Термины и определения», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698;

– Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», утвержденный Решением председателя Гостехкомиссии России от 30 марта 1992 г.

#### 4. ОСНОВНЫЕ ПОЛОЖЕНИЯ

4.1. В информационной системе «Образование» (далее – ИС «Образование») осуществляется обработка ПДн.

4.2. В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» (далее – МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы») при обработке ПДн необходимо принимать правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Мероприятия по обеспечению безопасности ПДн при их обработке в ИС «Образование» включают в себя определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз безопасности ПДн при их обработке в ИС «Образование» (далее – Модель угроз).

4.3. Модель угроз содержит систематизированный перечень угроз безопасности ПДн при их обработке в ИС «Образование».

4.4. Угрозы безопасности ПДн, содержащиеся в Модели угроз, могут уточняться и дополняться по мере развития способов и средств их реализации.

4.5. Настоящая Модель угроз сформирована в соответствии с методическими документами ФСТЭК России и ФСБ России с учетом следующих принципов:

– в случае обеспечения безопасности ПДн без использования СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России;

– в случае определения МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» необходимости обеспечения безопасности ПДн с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.

4.6. Модель угроз может быть пересмотрена:

– по решению МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИС «Образование»;

– по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИС «Образование»;

– в случае возникновения (обнаружения) новых уязвимостей и угроз безопасности ПДн;

– в случае изменения федерального законодательства в части определения угроз безопасности ПДн, актуальных при их обработке в ИСПДн;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности ПДн, которые будут актуальными для рассматриваемых типов ИСПДн;

- в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДн, следствием которого стало возникновение новых актуальных угроз безопасности ПДн;
- в случае повышения возможности реализации или опасности существующих угроз безопасности ПДн;
- в случае появления сведений и фактов о новых возможностях нарушителей.

## 5. ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОСОБЕННОСТЕЙ ЕЁ ФУНКЦИОНИРОВАНИЯ

### 5.1. Цели и задачи, решаемые ИС «Образование»

5.1.1. В ИС «Образование» в автоматизированном режиме обрабатываются ПДн в целях: выполнение возложенных законодательством Российской Федерации функций, полномочий и обязанностей в сфере образования, реализация иных уставных задач.

5.1.2. Перечень информации приведен в Приказе «Об утверждении перечня информационных систем персональных данных и перечня персональных данных, содержащихся в программных комплексах, входящих в состав информационных систем персональных данных в МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» от \_\_\_\_\_.

### 5.2. Описание структурно-функциональных характеристик ИС «Образование»

5.2.1. ИС «Образование» представляет собой локальную ИСПДн (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, объединенного в единую информационную систему в пределах одного здания), имеющую подключение к сетям связи, сети связи общего пользования и (или) сети «Интернет».

5.2.2. Логическими границами ИСПДн являются границы сети ИСПДн, выделенной на основе логического разделения сетей на оборудовании сетевой инфраструктуры МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы», реализующем функции управления (контроля) входящих в ИСПДн и исходящих из ИСПДн информационных потоков. Физические границы ИСПДн определены по периметрам помещений, в которых располагается ИСПДн.

5.2.3. Границы КЗ ИС «Образование» определяются Приказом «Об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных, и сохранности носителей ПДн в МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» от \_\_\_\_\_.

5.2.4. Общие характеристики ИС «Образование» приведены в таблице 1.

Таблица 1 – Характеристики ИС «Образование»

№ п/п	Характеристика	Значение характеристики
<b>Общие характеристики</b>		
1.	Состав ИС «Образование», программные комплексы	– Сетевой город; – Пакет офисных приложений Microsoft Office
2.	Место нахождения	– 424007, Республика Марий Эл, г. Йошкар-Ола, ул. Прохорова, д.48
3.	Назначение	Выполнение возложенных законодательством Российской Федерации функций, полномочий и обязанностей в сфере образования, реализация иных уставных задач
4.	Структура ИС «Образование»	Локальная
5.	Режим обработки ПДн в ИС «Образование»	Многопользовательский

№ п/п	Характеристика	Значение характеристики
6.	Разграничение прав доступа пользователей ИС «Образование»	С разграничением прав доступа
7.	Степень возможного ущерба при нарушении конфиденциальности информации	Высокая степень
8.	Степень возможного ущерба при нарушении доступности информации	Средняя степень
9.	Степень возможного ущерба при нарушении целостности информации	Средняя степень

5.2.5. Технические и эксплуатационные характеристики ИС «Образование», определяющие уровень исходной защищенности ИС «Образование», приведены в таблице 2.

Таблица 2 – Показатели исходной защищенности ИС «Образование»

№ п/п	Характеристика	Значение характеристики	Уровень защищенности
1.	Территориальное размещение	Локальная ИС, развернутая в пределах одного здания	Высокий
2.	Наличие соединения с сетями общего пользования	ИС, имеющая одноточечный выход в сеть общего пользования	Средний
3.	Встроенные (легальные) операции с записями баз данных	Чтение, поиск, запись, удаление, сортировка, модификация, передача	Низкий
4.	Разграничение доступа к данным	ИС, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИС	Средний
5.	Наличие соединений с базами данных иных ИС	ИС, в которой используется одна база данных, принадлежащая организации - владельцу данной ИС	Высокий
6.	Уровень обобщения (обезличивания) ПДн	ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
7.	Объем данных, которые предоставляются сторонним пользователям ИС «Образование» без предварительной обработки	ИС, предоставляющая часть данных	Средний

5.2.6. Соотношение характеристик ИС «Образование», соответствующих разным уровням защищенности, определенные на основании данных таблицы 2:

– 28.6% характеристик ИС «Образование» соответствуют *высокому* уровню защищенности;

– 42.9% характеристик ИС «Образование» соответствуют *среднему* уровню защищенности;

– 28.6% характеристик ИС «Образование» соответствуют *низкому* уровню защищенности.

5.2.7. В соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн, ИС «Образование» имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИС «Образование» соответствуют уровню «Высокий», а остальные – уровню «Средний». ИС «Образование» имеет средний уровень исходной защищенности, если не менее 70% характеристик ИС «Образование» соответствуют уровню не ниже «Средний», а остальные – уровню «Низкий». В остальных случаях ИС «Образование» имеет низкий уровень исходной защищенности. Уровень исходной защищенности ИС «Образование»: *средний* ( $Y_1=5$ ).

5.2.8. Перечень ПК, входящих в состав ИС «Образование», содержащих признаки обработки информации, и их характеристики приведены в таблице 3.

Таблица 3 – Характеристики программных комплексов в ИС «Образование»

№ п/п	Наименование ПК, содержащих признаки обработки информации	Категории ПДн, обрабатываемых в ПК	Категории субъектов ПДн, обрабатываемых в ПК	Количество субъектов ПДн, обрабатываемых в ПК	Тип угроз	Уровень защищенности ПДн, обрабатываемых в ПК
1.	Сетевой город	Иные	Субъекты, не являющиеся сотрудниками	Менее чем 100 000	Угрозы 3-го типа	4
2.	Пакет офисных приложений Microsoft Office	Иные	Субъекты, не являющиеся сотрудниками	Менее чем 100 000	Угрозы 3-го типа	4

5.2.9. Исходя из вышеуказанных характеристик ПК, входящих в состав ИС «Образование» и содержащих признаки обработки ПДн, для ПДн при их обработке в ИС «Образование» в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 определен 4 уровень защищенности. Основание: «Акт определения уровня защищенности персональных данных при их обработке в информационной системе «Образование» МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы» от \_\_\_\_\_.

5.2.10. Функциональные характеристики ИС «Образование» и используемые технологии отражены в таблице 4.

Таблица 4 – Функциональные характеристики и используемые технологии в ИС «Образование»

№ п/п	Характеристика	Значение характеристики
1.	Использование съемных носителей информации	Используются
2.	Использование технологий виртуализации	Используются
3.	Использование технологий беспроводного доступа	Используются

№ п/п	Характеристика	Значение характеристики
4.	Использование мобильных технических средств	Используются
5.	Использование веб-серверов	Не используются
6.	Использование Smart-карт	Не используются
7.	Использование облачных услуг	Не используются
8.	Использование GRID-систем	Не используются
9.	Использование технологий суперкомпьютерных систем	Не используются
10.	Использование хранилищ больших данных	Не используются
11.	Использование числового программного оборудования	Не используются
12.	Использование одноразовых паролей	Не используются
13.	Использование электронной почты	Используются
14.	Использование технологий передачи видеoinформации	Используются
15.	Использование технологий удаленного рабочего стола	Не используются
16.	Использование технологий удаленного администрирования	Не используются
17.	Использование технологий удаленного внеполосного доступа	Не используются
18.	Использование технологий веб-доступа	Не используются
19.	Использование технологий передачи речи	Не используются

#### 5.2.11. Состав ИС «Образование»:

- АРМ: 11.
- Серверы: 1.
- Коммутационное оборудование 3Com Switch 4500G 24-Port – 1.
- Сетевое хранилище данных (NAS) QNAP TS-853S Pro – 1.

### 5.3. Информационные потоки ИС «Образование»

5.3.1. МБОУ «Средняя общеобразовательная школа № 31 г.Йошкар-Олы» осуществляет передачу ПДн с использованием сетей общего пользования и (или) телекоммуникационных сетей международного информационного обмена. Особенности передачи ПДн в другие организации приведены в таблице 5.

Таблица 5 – Передача ПДн по открытым каналам связи в другие организации

Куда передается	Основания передачи	Субъекты ПДн	Категория субъекта ПДн
Образовательные учреждения Мурманской области	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Лица, не являющиеся сотрудниками организации	Привлекаемые эксперты; работники пункт проведения экзамена; участники государственной итоговой аттестации
Образовательные учреждения Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Лица, не являющиеся сотрудниками организации	Обучающиеся
Муниципальные образования Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Лица, не являющиеся сотрудниками организации	Привлекаемые эксперты; работники пункт проведения экзамена; участники государственной итоговой аттестации
Министерство образования и науки Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Лица, не являющиеся сотрудниками организации	Привлекаемые эксперты; работники пункт проведения экзамена; участники государственной

Куда передается	Основания передачи	Субъекты ПДн	Категория субъекта ПДн
			итоговой аттестации

5.3.2. МБОУ «Средняя общеобразовательная школа № 31 г.Йошкар-Олы» осуществляет передачу информации с использованием сетей общего пользования и (или) телекоммуникационных сетей международного информационного обмена. Особенности передачи информации в другие организации приведены в таблице 6.

Таблица 6 – Передача информации по открытым каналам связи в другие организации

Куда передается	Основания передачи	Перечень передаваемой информации
Образовательные учреждения Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Информация ограниченного доступа не содержащая сведений, составляющих государственную тайну
Муниципальные образования Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Информация ограниченного доступа не содержащая сведений, составляющих государственную тайну
Министерство образования и науки Чувашской Республики	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	Информация ограниченного доступа не содержащая сведений, составляющих государственную тайну

5.3.3. К информационным ресурсам ИС «Образование» не осуществляется удаленный доступ сотрудников других организаций.

5.3.4. Внутри организации в ИС «Образование» не осуществляется передача ПДн с использованием сетей связи общего пользования.

#### 5.4. Сети электросвязи ИС «Образование»

5.4.1. ИС «Образование» осуществляет взаимодействие с сетями электросвязи, описанными в таблице 7

Таблица 7 – Взаимодействие с сетями электросвязи

№ п/п	Категория сети электросвязи	Наименование оператора связи	Цель взаимодействия с сетью электросвязи	Способ взаимодействия с сетью электросвязи
1.	общего пользования	ПАО Ростелеком	оказание услуг	Тип доступа проводной, протоколы TCP/IP

#### 5.5. Объекты защиты ИС «Образование»

5.5.1. В соответствии с нормативными документами ФСБ России и ФСТЭК России к объектам защиты относятся:

- Персональные данные;
- Автоматизированные рабочие места пользователей;
- Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);

- Съемные машинные носители информации;
- Средства криптографической защиты информации (СКЗИ - программные, аппаратные);
  - Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;
  - Файлы конфигураций программного обеспечения и средств защиты информации;
  - Каналы (линии) связи, использующиеся для взаимодействия технических средств информационной системы, находящиеся в пределах контролируемых зон;
  - Эксплуатационная и техническая документация на СКЗИ;
  - Документация, в которой отражена информация о мерах и средствах защиты информационной системы;
- Помещения, в которых размещена информационная система.

## **6. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ИС «ОБРАЗОВАНИЕ»**

### **6.1. Описание потенциального нарушителя**

6.1.1. В соответствии с нормативными документами ФСТЭК России по наличию права постоянного или разового доступа в КЗ ИС «Образование» нарушители подразделяются на два типа:

– внешние нарушители – нарушители, не имеющие доступа к ИС «Образование», реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

– внутренние нарушители – нарушители, имеющие доступ к ИС «Образование», включая пользователей ИС «Образование», реализующие угрозы непосредственно в ИС «Образование».

6.1.2. В соответствии с нормативными документами ФСБ России все физические лица, имеющие доступ к техническим и программным средствам ИС «Образование», разделяются на следующие категории:

– лица, имеющие право постоянного доступа в контролируемую зону ИС «Образование» (сотрудники, имеющие доступ к ИС «Образование», зарегистрированные пользователи ИС «Образование» других организаций, обслуживающий персонал);

– лица, имеющие право разового доступа в контролируемую зону ИС «Образование» (посетители и обслуживающий персонал, лица, осуществляющие ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС «Образование», в том числе СЗИ);

– привилегированные пользователи ИС «Образование»;

– внешние источники атак.

6.1.3. Все потенциальные нарушители подразделяются на:

– внешних нарушителей, не имеющих доступа к ИС «Образование» и осуществляющих атаки из-за пределов контролируемой зоны ИС «Образование»;

– внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИС «Образование», включая пользователей ИС «Образование», и реализующих угрозы непосредственно в ИС «Образование».

6.1.4. Предполагается, что внешние источники атак, имеющие или не имеющие права доступа в контролируемую зону ИС «Образование», могут рассматриваться в качестве потенциальных источников атак.

6.1.5. Привилегированные пользователи – члены группы администраторов, которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств СКЗИ и СФ, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями. К их числу относятся ответственный за обеспечение безопасности ПДн в ИС «Образование» и ответственный пользователь криптосредств.

6.1.6. Предполагается, что обеспечивать безопасность ПДн с использованием

криптосредств необходимо только при передаче ПДн по каналам связи общего пользования, поэтому наличие потенциальных нарушителей возможно только среди категорий физических лиц, имеющих подключение к ИС «Образование».

6.1.7. Внешними нарушителями могут быть: 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; бывшие работники (пользователи).

6.1.8. Характер и объем ПДн, хранимых и обрабатываемых в ИС «Образование», является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных на утечку информации по ТКУИ.

6.1.9. Внутренними нарушителями могут быть: специальные службы иностранных государств (блоков государств); 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.

6.1.10. Исходя из целей и задач ИС «Образование», вида обрабатываемой информации, учета последствий от нарушений свойств безопасности информации, внутренних и внешних нарушители могут иметь следующие возможные цели (мотивацию) и возможности, описанные в таблице 8:

Таблица 8 – Цели внутренних и внешних нарушителей

Вид нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
<b>Внутренний нарушитель</b>	
Специальные службы иностранных государств (блоков государств)	– Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики; – Дискредитация или дестабилизация деятельности органов государственной власти, организаций
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	– Причинение имущественного ущерба путем мошенничества или иным преступным путем; – Непреднамеренные, неосторожные или неквалифицированные действия
Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	– Причинение имущественного ущерба путем мошенничества или иным преступным путем; – Непреднамеренные, неосторожные или неквалифицированные действия
Пользователи информационной системы	– Причинение имущественного ущерба путем мошенничества или иным преступным путем; – Любопытство или желание самореализации (подтверждение статуса); – Месть за ранее совершённые действия; – Непреднамеренные, неосторожные или неквалифицированные действия
Администраторы информационной системы и администраторы безопасности	– Причинение имущественного ущерба путем мошенничества или иным преступным путем;

<b>Вид нарушителя</b>	<b>Возможные цели (мотивация) реализации угроз безопасности информации</b>
	<ul style="list-style-type: none"> <li>– Любопытство или желание самореализации (подтверждение статуса);</li> <li>– Мечь за ранее совершённые действия;</li> <li>– Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;</li> <li>– Непреднамеренные, неосторожные или неквалифицированные действия</li> </ul>
<b>Внешний нарушитель</b>	
Специальные службы иностранных государств (блоков государств)	<ul style="list-style-type: none"> <li>– Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;</li> <li>– Дискредитация или дестабилизация деятельности органов государственной власти, организаций</li> </ul>
Террористические, экстремистские группировки	<ul style="list-style-type: none"> <li>– Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;</li> <li>– Совершение террористических актов;</li> <li>– Идеологические или политические мотивы;</li> <li>– Дискредитация или дестабилизация деятельности органов государственной власти, организаций</li> </ul>
Преступные группы (криминальные структуры)	<ul style="list-style-type: none"> <li>– Причинение имущественного ущерба путем мошенничества или иным преступным путем;</li> <li>– Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды</li> </ul>
Внешние субъекты (физические лица)	<ul style="list-style-type: none"> <li>– Идеологические или политические мотивы;</li> <li>– Причинение имущественного ущерба путем мошенничества или иным преступным путем;</li> <li>– Любопытство или желание самореализации (подтверждение статуса)</li> </ul>
Конкурирующие организации	<ul style="list-style-type: none"> <li>– Получение конкурентных преимуществ;</li> <li>– Причинение имущественного ущерба путем мошенничества или иным преступным путем</li> </ul>
Разработчики, производители, поставщики программных, технических и программно-технических средств	<ul style="list-style-type: none"> <li>– Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;</li> <li>– Причинение имущественного ущерба путем мошенничества или иным преступным путем;</li> <li>– Непреднамеренные, неосторожные или неквалифицированные действия</li> </ul>
Бывшие работники (пользователи)	<ul style="list-style-type: none"> <li>– Мечь за ранее совершённые действия;</li> <li>– Причинение имущественного ущерба путем мошенничества или иным преступным путем</li> </ul>

## 6.2. Предположения об информационной и технической вооруженности нарушителей

6.2.1. Внутренние нарушители могут иметь следующие возможности, описанные в таблице 9:

Таблица 9 – Возможности и цели внутренних нарушителей

<b>Вид внутреннего нарушителя</b>	<b>Возможности по реализации угроз безопасности информации</b>
Специальные службы иностран-	– Возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (не-

Вид внутреннего нарушителя	Возможности по реализации угроз безопасности информации
ных государств (блоков государств)	<p>защищенных организационными мерами);</p> <ul style="list-style-type: none"> <li>– 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;</li> <li>– Хорошая осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе;</li> <li>– 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;</li> <li>– Возможность создания методов и средств реализации угроз безопасности информации 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;</li> <li>– Возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему;</li> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– 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;</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы</li> </ul>
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	<ul style="list-style-type: none"> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	<ul style="list-style-type: none"> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Пользователи информационной	<ul style="list-style-type: none"> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных ис-</li> </ul>

Вид внутреннего нарушителя	Возможности по реализации угроз безопасности информации
системы	<p>точниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему;</p> <ul style="list-style-type: none"> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках</li> </ul>
Администраторы информационной системы и администраторы безопасности	<ul style="list-style-type: none"> <li>– 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;</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы;</li> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>

6.2.2. Внешние нарушители могут иметь следующие возможности, описанные в таблице 10:

Таблица 10 – Возможности и цели внутренних и внешних нарушителей

Вид внешнего нарушителя	Возможности по реализации угроз безопасности информации
Специальные службы иностранных государств (блоков государств)	<ul style="list-style-type: none"> <li>– Возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений;</li> <li>– Возможность создания методов и средств реализации угроз безопасности информации 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;</li> <li>– 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;</li> <li>– Хорошая осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе;</li> <li>– 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;</li> <li>– Возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами);</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свобод-</li> </ul>

Вид внешнего нарушителя	Возможности по реализации угроз безопасности информации
	<p>ном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения;</p> <ul style="list-style-type: none"> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках</li> </ul>
Террористические, экстремистские группировки	<ul style="list-style-type: none"> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– 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;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему;</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы</li> </ul>
Преступные группы (криминальные структуры)	<ul style="list-style-type: none"> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы;</li> <li>– 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;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Внешние субъекты (физические лица)	<ul style="list-style-type: none"> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Конкурирующие организации	<ul style="list-style-type: none"> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– 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 обеспе-</li> </ul>

Вид внешнего нарушителя	Возможности по реализации угроз безопасности информации
	<p>чения;</p> <ul style="list-style-type: none"> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Разработчики, производители, поставщики программных, технических и программно-технических средств	<ul style="list-style-type: none"> <li>– Осведомленность о мерах защиты информации, применяемых в информационной системе данного типа;</li> <li>– 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;</li> <li>– Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы;</li> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>
Бывшие работники (пользователи)	<ul style="list-style-type: none"> <li>– Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках;</li> <li>– Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему</li> </ul>

6.2.3. Предположение об отнесении внутренних нарушителей к потенциальным источникам атак описаны в таблице 11.

Таблица 11 – Возможные внутренние нарушители

Вид внутреннего нарушителя	Описание отнесения к числу потенциальных источников атак/ исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
Специальные службы иностранных государств (блоков государств)	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Съёмные машинные носители информации;</li> <li>– Средства криптографической защиты информации (СКЗИ - программные, аппаратные);</li> </ul>	Нет

Вид внутреннего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
		<ul style="list-style-type: none"> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации;</li> <li>– Каналы (линии) связи, используемые для взаимодействия технических средств информационной системы, находящиеся в пределах контролируемых зон;</li> <li>– Эксплуатационная и техническая документация на СКЗИ;</li> <li>– Документация, в которой отражена информация о мерах и средствах защиты информационной системы;</li> <li>– Помещения, в которых размещена информационная система</li> </ul>	
Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Цели (мотивация) предполагает потенциальное наличие нарушителя	<ul style="list-style-type: none"> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Средства криптографической защиты информации (СКЗИ - программные, аппаратные);</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации;</li> <li>– Каналы (линии) связи, используемые для взаимодействия технических средств информационной системы, находящиеся в пределах контролируемых зон;</li> <li>– Эксплуатационная и техническая документация на СКЗИ;</li> <li>– Помещения, в которых размещена информационная система</li> </ul>	Да
Лица, обеспечивающие функционирование информационных систем или обслуживания	Цели (мотивация) предполагает потенциальное наличие нарушителя	<ul style="list-style-type: none"> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Каналы (линии) связи, используемые для взаимодействия технических средств информаци-</li> </ul>	Да

Вид внутреннего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
ющие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)		<p>онной системы, находящиеся в пределах контролируемых зон;</p> <ul style="list-style-type: none"> <li>– Помещения, в которых размещена информационная система</li> </ul>	
Пользователи информационной системы	Цели (мотивация) предполагает потенциальное наличие нарушителя	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Съёмные машинные носители информации;</li> <li>– Средства криптографической защиты информации (СКЗИ - программные, аппаратные);</li> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации;</li> <li>– Каналы (линии) связи, использующиеся для взаимодействия технических средств информационной системы, находящиеся в пределах контролируемых зон;</li> <li>– Помещения, в которых размещена информационная система</li> </ul>	Да
Администраторы информационной системы и администраторы безопасности	<p>Ответственные лица назначаются из числа доверенных лиц;</p> <p>Проводятся работы по подбору персонала</p>	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Съёмные машинные носители информации;</li> <li>– Средства криптографической защиты информации (СКЗИ - программные, аппаратные);</li> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации;</li> <li>– Каналы (линии) связи, исполь-</li> </ul>	Нет

Вид внутреннего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
		<p>зующиеся для взаимодействия технических средств информационной системы, находящиеся в пределах контролируемых зон;</p> <ul style="list-style-type: none"> <li>– Эксплуатационная и техническая документация на СКЗИ;</li> <li>– Документация, в которой отражена информация о мерах и средствах защиты информационной системы;</li> <li>– Помещения, в которых размещена информационная система</li> </ul>	

6.2.4. Предположение об отнесении внешних нарушителей к потенциальным источникам атак описаны в таблице 12.

Таблица 12 – Возможные внешние нарушители

Вид внешнего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
Специальные службы иностранных государств (блоков государств)	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Съёмные машинные носители информации;</li> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации</li> </ul>	Нет
Террористические, экстремистские группировки	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Автоматизированные рабочие места пользователей;</li> <li>– Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства);</li> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> </ul>	Нет

Вид внешнего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
		– Файлы конфигураций программного обеспечения и средств защиты информации	
Преступные группы (криминальные структуры)	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес	– Персональные данные; – Автоматизированные рабочие места пользователей; – Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства); – Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию; – Файлы конфигураций программного обеспечения и средств защиты информации	Нет
Внешние субъекты (физические лица)	Цели (мотивация) предполагает потенциальное наличие нарушителя	– Персональные данные; – Автоматизированные рабочие места пользователей; – Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства); – Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию; – Файлы конфигураций программного обеспечения и средств защиты информации	Да
Конкурирующие организации	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес; Сфера деятельности организации не является не предполагает наличие конкурирующих организаций	– Персональные данные; – Автоматизированные рабочие места пользователей; – Серверная инфраструктура (сервера и обеспечивающее их функционирование оборудование и технические средства); – Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию; – Файлы конфигураций программного обеспечения и средств защиты информации	Нет
Разработчики, производители, поставщики прог-	Производятся работы по подбору программных, технических и программно-технических средств; Проводятся работы по подбору разработчиков, производителей и	– Файлы конфигураций программного обеспечения и средств защиты информации	Нет

Вид внешнего нарушителя	Описание отнесения к числу потенциальных источников атак/исключения из числа потенциальных источников атак	Объекты защиты, к которым нарушитель может иметь доступ	Предположение об отнесении нарушителей к потенциальным источникам атак
рамных, технических и программно-технических средств	поставщиков программных, технических и программно-технических средств		
Бывшие работники (пользователи)	Цели (мотивация) предполагает потенциальное наличие нарушителя	<ul style="list-style-type: none"> <li>– Персональные данные;</li> <li>– Информация, относящаяся к защите информации, включая ключевую, парольную и аутентифицирующую информацию;</li> <li>– Файлы конфигураций программного обеспечения и средств защиты информации</li> </ul>	Да

6.2.5. Потенциал нарушителя определяется мерой усилий, затраченных нарушителем при реализации угроз безопасности ПДн, обрабатываемых в ИС «Образование».

6.2.6. В зависимости от потенциала, требуемого для реализации угроз безопасности ПДн, обрабатываемых в ИС «Образование», нарушители подразделяются на:

- нарушителей, обладающих базовым (низким) потенциалом (возможности уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей).

- нарушителей, обладающих усиленным базовым (средним) потенциалом (возможности уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей).

- нарушителей, обладающих высоким потенциалом (возможности уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей).

6.2.7. Исходя из целей и задач ИС «Образование», характера и объема ПДн, хранимых и обрабатываемых в ИС «Образование», в качестве вероятных нарушителей рассматриваются: внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом.

6.2.8. В ИС «Образование» угрозы безопасности ПДн могут быть реализованы нарушителями следующими способами:

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах);

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на общесистемном уровне (операционные системы, гипервизоры);

- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на прикладном уровне (системы управления базами данных, браузеры, веб-приложения, иные прикладные программы общего и специального назначения);
- несанкционированный доступ к объектам защиты и (или) воздействие на объекты защиты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);
- несанкционированный физический доступ к объектам защиты и (или) воздействие на объекты защиты.

### 6.3. Обобщенные возможности источников атак

6.3.1. На основании исходных данных об ИС «Образование», объектах защиты и источниках атак определены обобщенные возможности источников атак, которые описаны в таблице 13:

Таблица 13 – Обобщенные возможности источников атак

Обобщенные возможности источников атак	Предположение о возможности источников атак
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

6.3.2. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности ПДн, обрабатываемых в ИС «Образование», определяется возможностями источников атак.

6.3.3. Анализ уточненных возможностей нарушителей и направления атак, исходя из обобщенных возможностей источников атак, приведен в Приложении № 1.

## **7. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИС «ОБРАЗОВАНИЕ»**

### **7.1. Общие положения**

7.1.1. В ИС «Образование» требуется обеспечить конфиденциальность, доступность и целостность защищаемой информации.

### **7.2. Угрозы безопасности в соответствии с нормативными документами ФСТЭК России**

7.2.1. В соответствии с нормативными документами ФСТЭК России возможно возникновение или умышленная реализация следующих групп угроз безопасности ПДн:

- угрозы утечки по техническим каналам;
- угрозы несанкционированного доступа к информации.

7.2.2. При обработке ПДн в ИС «Образование» за счет реализации ТКУИ возможно возникновение следующих угроз безопасности ПДн:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

7.2.3. Угрозы несанкционированного доступа к ПДн.

7.2.3.1. Угрозы непосредственного доступа к ПДн. Возможные угрозы непосредственного доступа:

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

– угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специальных программ для осуществления НСД;

- угрозы внедрения вредоносных программ (локально).

7.2.3.2. Угрозы удаленного доступа. Возможные угрозы удаленного доступа:

– анализ сетевого трафика с перехватом информации, передаваемой по локальной сети, а также во внешние сети и принимаемой из внешних сетей с помощью анализаторов пакетов («снифферы»);

– выявление паролей;

– подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;

– навязывание ложного маршрута сети путем несанкционированного использования протоколов маршрутизации;

- реализация отказа в обслуживании;
- удалённый запуск приложений;
- угрозы внедрения вредоносных программ (по сети).

### **7.3. Анализ возможных угроз**

7.3.1. В качестве исходного перечня возможных угроз безопасности ПДн используется банк данных угроз безопасности информации, сформированный ФСТЭК России (<http://bdu.fstec.ru/>).

7.3.2. Угрозы утечки информации по техническим каналам характеризуются высокой стоимостью оборудования, необходимого для их реализации, и высокой квалификацией нарушителя. Цели и задачи ИС «Образование», характер и объем ПДн, хранимых и обрабатываемых в ИС «Образование», являются недостаточными для мотивации нарушителя к реализации угроз, связанных с ТКУИ. Исходя из этого, в данной Модели угроз угрозы утечки информации по ТКУИ не рассматриваются.

7.3.3. Порядок доступа сотрудников МБОУ «Средняя общеобразовательная школа № 31 г.Йошкар-Олы» в помещения, в которых осуществляется обработка ПДн и размещены ИСПДн указан в Приказе «Об обеспечении безопасности помещений, в которых размещены информационные системы персональных данных, и сохранности носителей персональных данных в МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы».

7.3.4. Осуществляется разграничение прав доступа пользователей ИС «Образование». Правила разграничения прав доступа пользователей ИС «Образование» определены в Приказе «О системе разграничения доступа в информационных системах персональных данных».

7.3.5. Порядок, обеспечивающий сохранность используемых материальных носителей ПДн указан в Приказе «Об обеспечении безопасности материальных носителей персональных данных в МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы», их поэкземплярный учет ведется в Журнале учета материальных (отчуждаемых машинных) носителей персональных данных.

7.3.6. Требования к организации парольной защиты указаны в Приказе «О сотрудниках МБОУ «Средняя общеобразовательная школа № 31 г. Йошкар-Олы», осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну, и имеющих доступ к обрабатываемой информации, не содержащей сведения, составляющие государственную тайну».

7.3.7. По результатам рассмотрения структурно-функциональных характеристик ИС «Образование», применяемых информационных технологий, потенциала возможных нарушителей, класса защищенности ИС «Образование» и особенностей размещения ИС «Образование» из базового перечня угроз безопасности ПДн были исключены неприменимые угрозы. Перечень исключенных угроз безопасности ПДн с обоснованием приведен в Приложении № 2.

7.3.8. Перечень возможных угроз безопасности ПДн представлен в Приложении № 3.

7.3.9. Анализ возможных угроз безопасности ПДн приведен в Приложении № 4.

7.3.10. По каждому виду угрозы, экспертным путем (опрос специалистов) определена вероятность реализации угрозы (в виде вербальной градации показателя о

частоте (вероятности) реализации угрозы безопасности ПДн и соответствующего числового коэффициента  $Y_2$ ) в соответствии с правилами:

- 0 – для маловероятной угрозы;
- 2 – для низкой вероятности угрозы;
- 5 – для средней вероятности угрозы;
- 10 – для высокой вероятности угрозы.

7.3.11. С учетом полученных числовых коэффициентов  $Y_1$  и  $Y_2$  по каждому виду угрозы безопасности ПДн рассчитан числовой коэффициент реализуемости угрозы  $Y$  по формуле (1):

$$Y = (Y_1 + Y_2) / 20 \quad (1)$$

7.3.12. Вербальная интерпретация реализуемости конкретной угрозы безопасности ПДн определена в соответствии с правилами:

- если  $0 \leq Y \leq 0,3$ , то возможность реализации признается низкой;
- если  $0,3 < Y \leq 0,6$ , то возможность реализации признается средней;
- если  $0,6 < Y \leq 0,8$ , то возможность реализации признается высокой;
- если  $Y > 0,8$ , то возможность реализации признается очень высокой.

7.3.13. По каждому виду угрозы, экспертным путем (опрос специалистов) определена опасность (ущерб) в соответствии с правилами:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

7.3.14. При определении степени опасности угроз утечки информации по техническим каналам связи учитывались границы контролируемой зоны (КЗ) и размещение технических средств.

7.3.15. Определена актуальность угроз безопасности ПДн на основании коэффициента реализуемости угрозы ( $Y$ ) и показателя опасности угрозы по каждому ее виду, сделан вывод об актуальности угроз в соответствии с правилами в таблице 14.

Таблица 14 – Правила определения актуальности угрозы безопасности ПДн

Возможность реализации угрозы	Опасность угрозы		
	Низкая	Средняя	Высокая
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная
Очень высокая	Актуальная	Актуальная	Актуальная

## 8. ВЫВОДЫ

### 8.1. Актуальные угрозы безопасности ПДн

8.1.1. В результате анализа возможных угроз безопасности ПДн выявлено актуальных угроз безопасности: 84. Актуальные угрозы безопасности ПДн в ИС «Образование» приведены в таблице 15.

Таблица 15 – Актуальные угрозы безопасности ПДн в ИС «Образование»

№ п/п	Идентификатор угрозы	Угроза
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS
2.	УБИ.006	Угроза внедрения кода или данных
3.	УБИ.008	Угроза восстановления аутентификационной информации
4.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
5.	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной
6.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
7.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
8.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
9.	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
10.	УБИ.018	Угроза загрузки нештатной операционной системы
11.	УБИ.019	Угроза заражения DNS-кеша
12.	УБИ.022	Угроза избыточного выделения оперативной памяти
13.	УБИ.023	Угроза изменения компонентов системы
14.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
15.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
16.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
17.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
18.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
19.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
20.	УБИ.049	Угроза нарушения целостности данных кеша
21.	УБИ.053	Угроза невозможности управления правами пользователей BIOS
22.	УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
23.	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
24.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
25.	УБИ.069	Угроза неправомерных действий в каналах связи
26.	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
27.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
28.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации

29.	УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
30.	УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
31.	УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
32.	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам
33.	УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
34.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
35.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
36.	УБИ.088	Угроза несанкционированного копирования защищаемой информации
37.	УБИ.089	Угроза несанкционированного редактирования реестра
38.	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
39.	УБИ.091	Угроза несанкционированного удаления защищаемой информации
40.	УБИ.093	Угроза несанкционированного управления буфером
41.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
42.	УБИ.099	Угроза обнаружения хостов
43.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
44.	УБИ.103	Угроза определения типов объектов защиты
45.	УБИ.104	Угроза определения топологии вычислительной сети
46.	УБИ.108	Угроза ошибки обновления гипервизора
47.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
48.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
49.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
50.	УБИ.121	Угроза повреждения системного реестра
51.	УБИ.123	Угроза подбора пароля BIOS
52.	УБИ.124	Угроза подделки записей журнала регистрации событий
53.	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации
54.	УБИ.126	Угроза подмены беспроводного клиента или точки доступа
55.	УБИ.128	Угроза подмены доверенного пользователя
56.	УБИ.130	Угроза подмены содержимого сетевых ресурсов
57.	УБИ.133	Угроза получения сведений о владельце беспроводного устройства
58.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
59.	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
60.	УБИ.144	Угроза программного сброса пароля BIOS
61.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения
62.	УБИ.152	Угроза удаления аутентификационной информации
63.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
64.	УБИ.156	Угроза утраты носителей информации
65.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

66.	УБИ.158	Угроза форматирования носителей информации
67.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
68.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода
69.	УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
70.	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
71.	УБИ.170	Угроза неправомерного шифрования информации
72.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
73.	УБИ.172	Угроза распространения «почтовых червей»
74.	УБИ.174	Угроза «фарминга»
75.	УБИ.175	Угроза «фишинга»
76.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
77.	УБИ.179	Угроза несанкционированной модификации защищаемой информации
78.	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
79.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
80.	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
81.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
82.	УБИ.192	Угроза использования уязвимых версий программного обеспечения
83.	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
84.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем

8.1.2. Вероятность реализации угроз, связанных с наличием НДС в системном и прикладном программном обеспечении, экспертным путем определена маловероятной, ввиду обработки в ИС «Образование» информации, имеющей меньшую ценность (или стоимость), чем затраты на ее получение. Исходя из этого, угрозы 1-го и 2-го типа для данной ИС «Образование» не актуальны.

8.1.3. Выявленные актуальные угрозы безопасности ПДн в ИС «Образование» относятся к угрозам 3-го типа: угрозы, не связанные с наличием НДС в системном и прикладном программном обеспечении, используемом в ИС «Образование».

## **8.2. Уровень криптографической защиты информации**

8.2.1. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КСЗ.

8.2.2. В случае реализации комплекса мероприятий организационного и технического характера, снижающего вероятность реализации угроз со стороны внутренних нарушителей, допускается использование криптографических средств защиты класса КС1 и выше.

## ПРИЛОЖЕНИЕ № 1

## Анализ уточненных возможностей нарушителей и направления атак

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.	Проведение атаки при нахождении в пределах контролируемой зоны	Да	<ul style="list-style-type: none"> <li>– В помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц;</li> <li>– Обслуживающий персонал и лица, обеспечивающие функционирование ИС «Образование», имеют возможность находиться в помещениях, где расположена ИС «Образование», в отсутствие пользователей ИС «Образование»;</li> <li>– Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС «Образование», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн;</li> <li>– Ответственный за обеспечение безопасности ПДн, администраторы ИС «Образование» назначаются из числа особо доверенных лиц;</li> <li>– Работа пользователей ИС «Образование» и пользователей криптосредств регламентирована;</li> <li>– Проводится обучение пользователей ИС «Образование» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение;</li> <li>– Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются;</li> <li>– Используются сертифицированные средства защиты информации от НСД;</li> <li>– Ответственный пользователь криптосредств назначается из числа особо доверенных лиц</li> </ul>
2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных	Да	<ul style="list-style-type: none"> <li>– В помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц;</li> <li>– Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками;</li> <li>– Обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие</li> </ul>

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	действий		только для санкционированного прохода; – Корпуса системных блоков защищены от вскрытия (опечатаны/опломбированы)
3.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Нет	– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
4.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	Нет	– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности
5.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ	Нет	– Ответственный пользователь криптосредств назначается из числа особо доверенных лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками; – Документация на СКЗИ хранится у ответственного пользователя криптосредств в металлическом сейфе (шкафу); – Обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
6.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специали-	Нет	– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации воз-

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	зирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ		возможности. Высокая стоимость и сложность подготовки реализации возможности
7.	Возможность воздействовать на любые компоненты СКЗИ и СФ	Нет	– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
8.	Использование штатных средств ИС, ограниченные мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Да	<ul style="list-style-type: none"> <li>– Ответственный за обеспечение безопасности ПДн, администраторы ИС «Образование» назначаются из числа особо доверенных лиц;</li> <li>– Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС «Образование», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн;</li> <li>– Работа пользователей ИС «Образование» и пользователей криптосредств регламентирована;</li> <li>– Проводится обучение пользователей ИС «Образование» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение;</li> <li>– Не используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно не обновляются;</li> <li>– Используются сертифицированные средства защиты информации от НСД;</li> <li>– Программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по защите ПДн;</li> <li>– Пользователи ИСПДн не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн</li> </ul>
9.	Получение в рамках предоставленных полномочий, а также в резуль-	Нет	– Работа пользователей ИС «Образование» и пользователей криптосредств регламентирована;

№ п/п	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	тате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ		<ul style="list-style-type: none"> <li>– Проводится обучение пользователей ИС «Образование» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение;</li> <li>– Сведения о физических мерах защиты объектов, в которых размещена ИСПДн, доступны ограниченному кругу сотрудников</li> </ul>
10.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Да	<ul style="list-style-type: none"> <li>– Обслуживающий персонал и лица, обеспечивающие функционирование ИС «Образование», имеют возможность находиться в помещениях, где расположена ИС «Образование», в отсутствие пользователей ИС «Образование»;</li> <li>– В помещениях, в которых происходит обработка ПДн, возможно нахождение посторонних лиц;</li> <li>– Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками;</li> <li>– Обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода</li> </ul>
11.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Нет	<ul style="list-style-type: none"> <li>– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности. Высокая стоимость и сложность подготовки реализации возможности</li> </ul>
12.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Нет	<ul style="list-style-type: none"> <li>– Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности</li> </ul>



## ПРИЛОЖЕНИЕ № 2

## Перечень исключенных угроз безопасности ПДн

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
1.	УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Грид-системы не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
2.	УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Грид-системы не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы
3.	УБИ.003	Угроза анализа криптографических алгоритмов и их реализации	Потенциал внешнего нарушителя недостаточен для реализации угрозы
4.	УБИ.005	Угроза внедрения вредоносного кода в BIOS	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
5.	УБИ.007	Угроза воздействия на программы с высокими привилегиями	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
6.	УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
7.	УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы
8.	УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Оператор не является поставщиком облачных услуг
9.	УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Оператор не является потребителем облачных услуг
10.	УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Потенциал внутреннего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
11.	УБИ.025	Угроза изменения системных и глобальных переменных	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
12.	УБИ.026	Угроза искажения XML-схемы	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
13.	УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Суперкомпьютеры не используются
14.	УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Потенциал внешнего нарушителя недостаточен для реализации угрозы
15.	УБИ.033	Угроза использования слабостей кодирования входных данных	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
16.	УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Потенциал внешнего нарушителя недостаточен для реализации угрозы
17.	УБИ.036	Угроза исследования механизмов работы программы	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
18.	УБИ.037	Угроза исследования приложения через отчёты об ошибках	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
19.	УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Технологии больших данных не используются
20.	УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Потенциал внешнего нарушителя недостаточен для реализации угрозы
21.	УБИ.040	Угроза конфликта юрисдикций различных стран	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг
22.	УБИ.041	Угроза межсайтового скриптинга	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Веб-серверы не используются; Веб-доступ не используется

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
23.	УБИ.042	Угроза межсайтовой подделки запроса	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Веб-серверы не используются; Веб-доступ не используется; Потенциал внешнего нарушителя недостаточен для реализации угрозы
24.	УБИ.043	Угроза нарушения доступности облачного сервера	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг
25.	УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
26.	УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Грид-системы не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
27.	УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
28.	УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Технологии больших данных не используется
29.	УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Оператор не является потребителем облачных услуг
30.	УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Оператор не является потребителем облачных услуг
31.	УБИ.055	Угроза незащищённого администрирования облачных услуг	Оператор не является потребителем облачных услуг
32.	УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Оператор не является потребителем облачных услуг
33.	УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Технологии больших данных не используется
34.	УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Оператор не является потребителем облачных услуг
35.	УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Технологии больших данных не используется
36.	УБИ.061	Угроза некорректного задания структуры данных транзакции	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
37.	УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
38.	УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг
39.	УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Оператор не является потребителем облачных услуг
40.	УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Оператор не является потребителем облачных услуг
41.	УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
42.	УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
43.	УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
44.	УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
45.	УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
46.	УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
47.	УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Грид-системы не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы
48.	УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Суперкомпьютеры не используются; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
49.	УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
50.	УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Технология удаленного внеполосного доступа не используется; Потенциал внешнего нарушителя недостаточен для реализации угрозы
51.	УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Угроза нехарактерна для данного типа системы; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
52.	УБИ.095	Угроза несанкционированного управления указателями	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
53.	УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Оператор не является потребителем облачных услуг
54.	УБИ.097	Угроза несогласованности правил доступа к большим данным	Технологии больших данных не используется
55.	УБИ.101	Угроза общедоступности облачной инфраструктуры	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг; Потенциал внешнего нарушителя недостаточен для реализации угрозы
56.	УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
57.	УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Технологии больших данных не используется
58.	УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Суперкомпьютеры не используется
59.	УБИ.107	Угроза отключения контрольных датчиков	Угроза нехарактерна для данного типа системы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
60.	УБИ.109	Угроза перебора всех настроек и параметров приложения	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
61.	УБИ.110	Угроза перегрузки GRID-системы вычислительными заданиями	GRID-системы не используются
62.	УБИ.111	Угроза передачи данных по скрытым каналам	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
63.	УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Угроза нехарактерна для данного типа системы; Числовое программное оборудование не используется
64.	УБИ.114	Угроза переполнения целочисленных переменных	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
65.	УБИ.117	Угроза перехвата привилегированного потока	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
66.	УБИ.118	Угроза перехвата привилегированного процесса	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
67.	УБИ.119	Угроза перехвата управления гипервизором	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
68.	УБИ.120	Угроза перехвата управления средой виртуализации	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
69.	УБИ.122	Угроза повышения привилегий	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
70.	УБИ.127	Угроза подмены действия пользователя путём обмана	Потенциал внешнего нарушителя недостаточен для реализации угрозы
71.	УБИ.131	Угроза подмены субъекта сетевого доступа	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы
72.	УБИ.132	Угроза получения предварительной информации об объекте защиты	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы
73.	УБИ.134	Угроза потери доверия к поставщику облачных услуг	Оператор не является потребителем облачных услуг; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
74.	УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Оператор не является потребителем облачных услуг
75.	УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Технологии больших данных не используется
76.	УБИ.137	Угроза потери управления облачными ресурсами	Оператор не является потребителем облачных услуг; Потенциал внешнего нарушителя недостаточен для реализации угрозы
77.	УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Оператор не является потребителем облачных услуг; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
78.	УБИ.139	Угроза преодоления физической защиты	Потенциал внешнего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
79.	УБИ.141	Угроза привязки к поставщику облачных услуг	Оператор не является потребителем облачных услуг
80.	УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Оператор не является поставщиком облачных услуг; Оператор не является потребителем облачных услуг; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
81.	УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Суперкомпьютеры не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
82.	УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Грид-системы не используются; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
83.	УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Технологии больших данных не используется
84.	УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
85.	УБИ.150	Угроза сбоя процесса обновления BIOS	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
86.	УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Веб-серверы не используются
87.	УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
88.	УБИ.159	Угроза «форсированного веб-браузинга»	Веб-доступ не используется
89.	УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Суперкомпьютеры не используются
90.	УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
91.	УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Оператор не является поставщиком облачных услуг
92.	УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
93.	УБИ.166	Угроза внедрения системной избыточности	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
94.	УБИ.169	Угроза наличия механизмов разработчика	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
95.	УБИ.173	Угроза «спама» веб-сервера	Веб-серверы не используются

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
96.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Угроза нехарактерна для данного типа системы
97.	УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Одноразовые пароли не используется; Потенциал внешнего нарушителя недостаточен для реализации угрозы
98.	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Угроза нехарактерна для данного типа системы; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
99.	УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
100.	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
101.	УБИ.188	Угроза подмены программного обеспечения	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
102.	УБИ.189	Угроза маскирования действий вредоносного кода	Потенциал внешнего нарушителя недостаточен для реализации угрозы
103.	УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы
104.	УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Потенциал внешнего нарушителя недостаточен для реализации угрозы
105.	УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Потенциал внешнего нарушителя недостаточен для реализации угрозы
106.	УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
107	УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Потенциал внешнего нарушителя недостаточен для реализации угрозы
108	УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
109	УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы
110	УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Потенциал внешнего нарушителя недостаточен для реализации угрозы
111	УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Потенциал внешнего нарушителя недостаточен для реализации угрозы
112	УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Веб-серверы не используются; Потенциал внешнего нарушителя недостаточен для реализации угрозы
113	УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Потенциал внешнего нарушителя недостаточен для реализации угрозы
114	УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
115	УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Угроза нехарактерна для данного типа системы; Потенциал внешнего нарушителя недостаточен для реализации угрозы
116	УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Угроза нехарактерна для данного типа системы; Числовое программное оборудование не используется; Потенциал внешнего нарушителя недостаточен для реализации угрозы
117	УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Угроза нехарактерна для данного типа системы; Числовое программное оборудование не используется

№ п/п	Идентификатор угрозы	Наименование угрозы	Обоснование исключения
118	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Не осуществляется удалённый доступ сотрудников других организаций к ИС; Нет передачи внутри организации с использованием сетей связи общего пользования; Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы
119	УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
120	УБИ.212	Угроза перехвата управления информационной системой	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
121	УБИ.213	Угроза обхода многофакторной аутентификации	Потенциал внешнего нарушителя недостаточен для реализации угрозы
122	УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
123	УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Потенциал внутреннего нарушителя недостаточен для реализации угрозы
124	УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	В системе не используются Smart-карты; Потенциал внешнего нарушителя недостаточен для реализации угрозы
125	УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Потенциал внешнего нарушителя недостаточен для реализации угрозы; Потенциал внутреннего нарушителя недостаточен для реализации угрозы

## ПРИЛОЖЕНИЕ № 3

## Перечень возможных угроз безопасности ПДн

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
1.	УБИ.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	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
2.	УБИ.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 поль-	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			зователя 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)				
3.	УБИ.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 так-	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			же в некоторых случаях – «вручную»				
4.	УБИ.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): 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 осуществ-	Микропрограммное обеспечение BIOS/UEFI	Внутренний разрушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			вляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию				
5.	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной	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	Сетевой узел	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
6.	УБИ.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 контро-	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение,	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ля 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	метаданные, объекты файловой системы, реестр			уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
7.	УБИ.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	Микропрограммное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации				
8.	УБИ.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 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	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
9.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пу-	Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных	Объекты файловой системы	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		ти	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				(или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
10.	УБИ.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	Прикладное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				
11.	УБИ.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	Микропрограммное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах))
12.	УБИ.019	Угроза заражения DNS-кеша	Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и домен-	Сетевой узел, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ных 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. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу				
13.	УБИ.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 обеспе-	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое обо-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			чения в системе в активном состоянии				рудование, сетевые приложения, сервисы)
14.	УБИ.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 файлам, 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	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
15.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение,	Внешний нарушитель с высоким потенциалом, внутренний нарушитель с низким потенциалом	Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		информации	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	аппаратное обеспечение			доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, webприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
16.	УБИ.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	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, webприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				рованный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
17.	УБИ.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 произ-	Средства защиты информации, системное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	Внешний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			водителя/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				
18.	УБИ.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	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
19.	УБИ.034	Угроза использования	Угроза заключается в возможности осуществления на-	Системное программное обеспе-	Внешний нарушитель с низким по-	Конфиденциальность	Несанкционированный доступ и (или) воздействие на

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		слабостей протоколов сетевого/локального обмена данными	рушителем 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	чение, сетевое программное обеспечение, сетевой трафик	тенциалом, внутренним нарушителем с низким потенциалом		объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
20.	УБИ.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 обновле-	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>ния, 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</p>				
21.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	<p>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</p>	Сетевой узел, сетевое программное обеспечение, метаданные, учётные данные пользователя	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия				
22.	УБИ.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. 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)	Сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
23.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при	Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компь-	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой	Внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		выводе из промежуточных состояний питания	ютере. 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.)	системы, реестр			доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
24.	УБИ.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	Микропрограммное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах))
25.	УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычисли-	Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных	Информационная система, сервер	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		тельных ресурсов	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 виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями				(или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
26.	УБИ.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	Сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			результате реализации угрозы межсайтового скриптинга				
27.	УБИ.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.	Аппаратное обеспечение, носители информации, объекты файловой системы	Внутренний нарушитель с низким потенциалом	Конфиденциальность	Воздействие на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
28.	УБИ.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	Сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность Целостность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				
29.	УБИ.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 но-	Машинный носитель информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>сителя 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</p>				
30.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	<p>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:</p>	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Внутренний разрушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера				
31.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Угроза заключается в возможности извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
32.	УБИ.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.	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (систе-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>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). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации</p>				<p>мы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>
33.	УБИ.078	<p>Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети</p>	<p>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 вир-</p>	Виртуальная машина	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	<p>Конфиденциальность Целостность Доступность</p>	<p>Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			туальной машины на момент осуществления нарушителем деструктивного программного воздействия				
34.	УБИ.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, реализованных 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	Виртуальная машина	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
35.	УБИ.083	Угроза несанкционированного доступа к системе по беспровод-	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), не-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		ным каналам	каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2, AES), используемых для доступа к беспроводному оборудованию. 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				санкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
36.	УБИ.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 рас-	Виртуальные устройства хранения данных, виртуальные диски	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложе-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>пределения 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 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.)</p>				<p>ния, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>
37.	УБИ.086	Угроза несанкционированного изменения аутентификационной ин-	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специ-	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		формации	альных 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				(или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
38.	УБИ.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	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом, внешний нарушитель с высоким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
39.	УБИ.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). Дан-	Объекты файловой системы, машинный носитель информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные прог-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ная 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				раммы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
40.	УБИ.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 реес-	Системное программное обеспечение, использующее реестр, реестр	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			тром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра				
41.	УБИ.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)	Системное программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
42.	УБИ.091	Угроза несанкционированного	Угроза заключается в возможности причинения наруши-	Метаданные, объекты файловой	Внешний нарушитель с низким по-	Доступность	Несанкционированный доступ и (или) воздействие на

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		рованного удаления защищаемой информации	телем 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 расстоянии, достаточное для оказания эффективного деструктивного воздействия	системы, реестр	тенциалом, внутренним нарушителем с низким потенциалом		объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
43.	УБИ.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, переполне-	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами дан-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>ние 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</p>				<p>ных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>
44.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	<p>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</p>	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	<p>Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ми 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 Источники угрозы Внешний нарушитель с низким потенциалом				
45.	УБИ.099	Угроза об-наружения 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	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика				
46.	УБИ.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	Системное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
47.	УБИ.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	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложе-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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 межсетевое 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.)				ния, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
48.	УБИ.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	Сетевой узел, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложе-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				ния, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
49.	УБИ.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.	Системное программное обеспечение, гипервизор	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоях 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</p>				
50.	УБИ.113	<p>Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники</p>	<p>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</p>	<p>Системное программное обеспечение, аппаратное обеспечение</p>	<p>Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом</p>	<p>Целостность Доступность</p>	<p>Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации</p>

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			физической возможности) на осуществление форсированной перезагрузки				
51.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Угроза заключается в возможности осуществления 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,	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			содержащих защищаемую информацию) и др.				
52.	УБИ.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 вычислительной сети; неспособность технологий, с помощью	Сетевой узел, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных				
53.	УБИ.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, возникновение 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 воз-	Объекты файловой системы, реестр	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			можно 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				
54.	УБИ.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	Микропрограммное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
55.	УБИ.124	Угроза подделки записей журналов	Угроза заключается в возможности внесения нарушителем изменений в журналы регистра-	Системное программное обеспечение	Внешний нарушитель с низким потенциалом, внут-	Целостность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		нала регистрации событий	ции событий безопасности дискредитируемой системы (удаление компрометирующих 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		ренний нарушитель с низким потенциалом		уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
56.	УБИ.125	Угроза подключения к	Угроза заключается в возможности осуществления на-	Сетевой узел, сетевое програм-	Внешний нарушитель с низким по-	Конфиденциальность	Несанкционированный доступ и (или) воздействие на

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		беспроводной сети в обход процедуры аутентификации	рушителем 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	мное обеспечение	тенциалом	Целостность Доступность	объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
57.	УБИ.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 воз-	Сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка беспроводного доступа	Внешний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			можно 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				
58.	УБИ.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.	Сетевой узел, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
59.	УБИ.129	Угроза подмены резервной копии программ	Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Внутренний нарушитель с низким потенциалом	Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрог-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		многообеспечения BIOS	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)				раммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
60.	УБИ.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	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				
61.	УБИ.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 дан-	Сетевой узел, метаданные	Внешний нарушитель с низким потенциалом	Конфиденциальность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ным стационарных точек беспроводного доступа, с которыми в автоматическом режиме осуществляет взаимодействие беспроводное устройство дискредитируемого пользователя				
62.	УБИ.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 или при использовании недостатков реализации сетевых протоколов. 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 и ошибками реализации сетевых протоколов. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы или наличия ошибок реализации сетевых протоколов (например, формирование IP-адреса версии 6 на основе MAC-	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик, телекоммуникационное устройство	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, webприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			адреса, определение доступности IP-адреса, использование функции контроля целостности PPP-интерфейса и др.)				
63.	УБИ.143	Угроза программного вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Угроза заключается в возможности прерывания носителем 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 перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации, а также невозможности длительного нахождения средств хранения, обработки и (или) ввода/вывода/передачи информации в ре-	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение, телекоммуникационное устройство	Внешний нарушитель со средним потенциалом, внешний нарушитель с низким потенциалом, внутренний нарушитель со средним потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>жиге предельно допустимых значений (частота системной шины, центрального процессора, количества обращений на чтение и/или запись и другие параметры). 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</p>				
64.	УБИ.144	Угроза программного сброса пароля BIOS	<p>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. 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</p>	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			установки и запуска данных средств				
65.	УБИ.145	Угроза пропуски 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	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), воздействие на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); »автоматического метода» – нарушитель осуществляет деструктивное воздействие перенадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер				
66.	УБИ.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	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			использование данных средств; нарушитель обладает специальным программным обеспечением, реализующим функцию сброса аутентификационной информации, и получил привилегии в дискредитируемой системе на использование данных средств				
67.	УБИ.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 объемом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объем 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 сторон-	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			них серверах с недостаточными мерами контроля подлинности сетевых запросов; сведений о сетевом адресе дискредитируемой системы; специального программного обеспечения, реализующего функции генерации сетевых пакетов				
68.	УБИ.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»	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				
69.	УБИ.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	Носитель информации	Внутренний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
70.	УБИ.157	Угроза физического	Угроза заключается в возможности умышленного выведе-	Сервер, рабочая станция, носитель	Внешний нарушитель с низким по-	Целостность Доступность	Несанкционированный физический доступ и (или) воз-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ния из строя внешним нарушителем средств хранения, обработки 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.)	информации, аппаратное обеспечение	тенциалом		действие на линии, (каналы) связи, технические средства, машинные носители информации
71.	УБИ.158	Угроза форматирования носителей информации	Угроза заключается в возможности утраты хранящейся на форматированном 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	Носитель информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные прог-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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.				раммы общего и специального назначения)
72.	УБИ.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.)	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
73.	УБИ.162	Угроза эксплуатации цифровой	Угроза заключается в возможности повышения нарушителем привилегий в системах, ис-	Системное программное обеспечение, прикладное	Внешний нарушитель с низким потенциалом, внут-	Конфиденциальность Целостность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		подписи программного кода	пользующих 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	программное обеспечение	внешний нарушитель с низким потенциалом	Доступность	на уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
74.	УБИ.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.	Сетевой узел, сетевое программное обеспечение	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные прог-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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 неблагоприятным содержанием				раммы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
75.	УБИ.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	Сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Доступность	Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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				
76.	УБИ.170	Угроза неравномерного 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	Объект файловой системы	Внешний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
77.	УБИ.171	Угроза скрытого включения вычислительного ус-	Угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с мно-	Сетевой узел, сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры,

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		тройства в состав бот-сети	жества 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				операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
78.	УБИ.172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми на компьютер	Сетевое программное обеспечение	Внешний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры,

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>ливаемыми 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</p>				<p>операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)</p>
79.	УБИ.174	Угроза «фарминга»	<p>Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём скрытого 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</p>	Рабочая станция, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	<p>Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое обо-</p>

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			<p>конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; средств создания и запуска поддельного сайта; 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</p>				<p>рудование, сетевые приложения, сервисы)</p>
80.	УБИ.175	Угроза «фишинга»	<p>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</p>	Рабочая станция, сетевое программное обеспечение, сетевой трафик	Внешний нарушитель с низким потенциалом	Конфиденциальность	<p>Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)</p>

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			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)				
81.	УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопас-	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.	Системное программное обеспечение, сетевое программное обеспечение, рикладное программное обеспечение, аппаратное обеспечение	Внутренний нарушитель с низким потенциалом	Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		ностью	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				уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
82.	УБИ.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 се-	Системное программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами дан-

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			тевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях: 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				ных, браузеры, webприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
83.	УБИ.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 расстоянии, достаточное для оказания эффективного деструктивного воздействия	Объекты файловой системы	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Целостность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
84.	УБИ.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	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	Внутренний нарушитель с низким потенциалом, внешний нарушитель со средним потенциалом	Доступность	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
85.	УБИ.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, коррозионных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями техничес-	Аппаратное средство	Внутренний нарушитель с низким потенциалом	Доступность	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ких средств в условиях, не удовлетворяющих требованиям заданных их производителем				
86.	УБИ.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	Средство защиты информации	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
87.	УБИ.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 обус-	Сетевое программное обеспечение	Внутренний нарушитель с низким потенциалом	Целостность Доступность	Воздействие на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия)

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ловлена 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				
88.	УБИ.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	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
89.	УБИ.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 ме-	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			ханизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей				(или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы)
90.	УБИ.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	Аппаратное устройство, программное обеспечение	Внешний нарушитель с низким потенциалом	Доступность	Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения)
91.	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Угроза заключается в возможности получения доступа к защищенной памяти из программы, не обладающей соответствующими правами, в результате эксплуатации уязвимостей, позволяющих преодолеть механизм разграничения доступа, реализу-	Аппаратное устройство	Внешний нарушитель с низким потенциалом, внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность Доступность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
			емый центральным процессором. Реализация данной угрозы обусловлена наличием уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении инструкций процессора. Ошибка контроля доступа обусловлена следующими факторами: 1) отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти; 2) отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения; 3) хранение данных ядра операционной системы в адресном пространстве процесса. Реализация данной угрозы возможна из-за наличия процессоров, имеющих аппаратные уязвимости и отсутствия соответствующих обновлений				объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы)
92.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла,	Угроза заключается в возможности деструктивного воздействия на информационную систему и обрабатываемую ею информацию в результате работы программного обеспечения, используемого для администрирования информационных систем. Данная угроза связана со слабостями процедуры проверки	Системное программное обеспечение	Внутренний нарушитель с низким потенциалом	Конфиденциальность Целостность	Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах)), несанкционированный доступ и (или) воздействие на объекты на общесистемном уровне (базовые системы

№ п/п	Идентификатор угрозы	Наименование угрозы	Описание	Объект воздействия	Источник угрозы	Нарушаемое свойство безопасности	Способ реализации
		используемого программного обеспечением администрирования информационных систем	пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования информационных систем. Реализация данной угрозы возможна в случае, если в информационной системе используется программное обеспечение администрирования информационных систем, которое в качестве исходных данных использует конфигурационные файлы, сформированные на основе пользовательских данных				ввода-вывода, гипервизоры, операционные системы), несанкционированный доступ и (или) воздействие на объекты на прикладном уровне (системы управления базами данных, браузеры, вебприложения, иные прикладные программы общего и специального назначения), несанкционированный доступ и (или) воздействие на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы), несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации

ПРИЛОЖЕНИЕ № 4  
Определение актуальности угроз безопасности ПДн

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
2.	УБИ.006	Угроза внедрения кода или данных	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
3.	УБИ.008	Угроза восстановления аутентификационной информации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
4.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да
5.	УБИ.011	Угроза деавторизации санкционированного клиента беспроводной	средний (5)	низкая (2)	средняя (0.35)	средняя	Да
6.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
7.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
8.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	средний (5)	низкая (2)	средняя (0.35)	средняя	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
9.	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
10.	УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
11.	УБИ.018	Угроза загрузки нештатной операционной системы	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
12.	УБИ.019	Угроза заражения DNS-кеша	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
13.	УБИ.022	Угроза избыточного выделения оперативной памяти	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
14.	УБИ.023	Угроза изменения компонентов системы	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
15.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
16.	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
17.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	средний (5)	высокая (10)	высокая (0.75)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
18.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
19.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
20.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
21.	УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
22.	УБИ.049	Угроза нарушения целостности данных кеша	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
23.	УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
24.	УБИ.053	Угроза невозможности управления правами пользователей BIOS	средний (5)	средняя (5)	средняя (0.5)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
25.	УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	средний (5)	средняя (5)	средняя (0.5)	средняя	Да
26.	УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
27.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
28.	УБИ.069	Угроза неправомерных действий в каналах связи	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
29.	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
30.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
31.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
32.	УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
33.	УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
34.	УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
35.	УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
36.	УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
37.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
38.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да
39.	УБИ.088	Угроза несанкционированного копирования защищаемой информации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
40.	УБИ.089	Угроза несанкционированного редактирования реестра	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
41.	УБИ.090	Угроза несанкционированного создания учётной записи пользователя	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
42.	УБИ.091	Угроза несанкционированного удаления защищаемой информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
43.	УБИ.093	Угроза несанкционированного управления буфером	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
44.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
45.	УБИ.099	Угроза обнаружения хостов	средний (5)	высокая (10)	высокая (0.75)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
46.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
47.	УБИ.103	Угроза определения типов объектов защиты	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
48.	УБИ.104	Угроза определения топологии вычислительной сети	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
49.	УБИ.108	Угроза ошибки обновления гипервизора	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
50.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	средний (5)	низкая (2)	средняя (0.35)	средняя	Да
51.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
52.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
53.	УБИ.121	Угроза повреждения системного реестра	средний (5)	средняя (5)	средняя (0.5)	средняя	Да
54.	УБИ.123	Угроза подбора пароля BIOS	средний (5)	высокая (10)	высокая (0.75)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
55.	УБИ.124	Угроза подделки записей журнала регистрации событий	средний (5)	средняя (5)	средняя (0.5)	средняя	Да
56.	УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
57.	УБИ.126	Угроза подмены беспроводного клиента или точки доступа	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
58.	УБИ.128	Угроза подмены доверенного пользователя	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
59.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
60.	УБИ.130	Угроза подмены содержимого сетевых ресурсов	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
61.	УБИ.133	Угроза получения сведений о владельце беспроводного устройства	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да
62.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	средний (5)	средняя (5)	средняя (0.5)	средняя	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
63.	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	средний (5)	низкая (2)	средняя (0.35)	средняя	Да
64.	УБИ.144	Угроза программного сброса пароля BIOS	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
65.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
66.	УБИ.152	Угроза удаления аутентификационной информации	средний (5)	средняя (5)	средняя (0.5)	высокая	Да
67.	УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	средний (5)	средняя (5)	средняя (0.5)	средняя	Да
68.	УБИ.155	Угроза утраты вычислительных ресурсов	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
69.	УБИ.156	Угроза утраты носителей информации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
70.	УБИ.157	Угроза физического вывода из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
71.	УБИ.158	Угроза форматирования носителей информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
72.	УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
73.	УБИ.162	Угроза эксплуатации цифровой подписи программного кода	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да
74.	УБИ.167	Угроза заражения компьютера при посещении неблагонядёжных сайтов	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
75.	УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
76.	УБИ.170	Угроза неправомерного шифрования информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
77.	УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	средний (5)	высокая (10)	высокая (0.75)	средняя	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
78.	УБИ.172	Угроза распространения «почтовых червей»	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
79.	УБИ.174	Угроза «фарминга»	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
80.	УБИ.175	Угроза «фишинга»	средний (5)	высокая (10)	высокая (0.75)	высокая	Да
81.	УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
82.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
83.	УБИ.179	Угроза несанкционированной модификации защищаемой информации	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
84.	УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	средний (5)	средняя (5)	средняя (0.5)	средняя	Да
85.	УБИ.182	Угроза физического устаревания аппаратных компонентов	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
86.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	средний (5)	низкая (2)	средняя (0.35)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
87.	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	средний (5)	высокая (10)	высокая (0.75)	средняя	Да
88.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да
89.	УБИ.192	Угроза использования уязвимых версий программного обеспечения	средний (5)	низкая (2)	средняя (0.35)	высокая	Да
90.	УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	средний (5)	маловероятно (0)	низкая (0.25)	средняя	Нет
91.	УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	средний (5)	низкая (2)	средняя (0.35)	высокая	Да

№ п/п	Идентификатор угрозы	Наименование угрозы	Уровень исходной защищенности (Y1)	Вероятность (Y2)	Возможность реализации (Y)	Опасность	Актуальность
92.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	средний (5)	маловероятно (0)	низкая (0.25)	высокая	Да