Автономное учреждение профессионального образования
Ханты-Мансийского автономного округа - Югры
«НЕФТЕЮГАНСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»
(АУ «Нефтеюганский политехнический колледж»)
сокращенное название организации

ПРИКАЗ

18.11.2022 № 01-01-06/567

Об утверждении моделей угроз персональных данных в информационных системах АУ "Нефтеюганский политехнический колледж"

В соответствии с Федеральным законом от 27.07.2006 года №152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 №1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

ПРИКАЗЫВАЮ:

1. Утвердить Модель угроз безопасности персональных данных в информационной системе «Бухгалтерский и кадровый учет» в АУ «Нефтеюганский политехнический колледж» (Приложение 1).
2. Утвердить Модель угроз безопасности персональных данных в информационной системе «1С Колледж проф» (Приложение 2).
3. Утвердить Модель угроз безопасности персональных данных в информационной системе «Сайт» (Приложение 3).
4. Заведующему отделу информационных технологий (Бутко Д.Н.) опубликовать на сайте колледжа документы, указанные в пунктах 1-3 настоящего приказа в срок до 25.11.2022.
5. Контроль за исполнением приказа оставляю за собой.

Директор М.В. Гребенец

Исполнитель:
Анастасия Олеговна Иванова
Специалист по кадрам
iao@neftpk.ru
+7 (3463) 200-995, доб. 150

Лист ознакомления к приказу
№ 01-01-06/567 от 18.11.2022

С приказом № 01-01-06/567 от 18.11.2022 «Об утверждении моделей угроз персональных данных в информационных системах АУ "Нефтеюганский политехнический колледж"»

ОЗНАКОМЛЕН:

Бутко Денис Николаевич _____ 18.11.2022

Утверждена приказом АУ
«Нефтеюганский политехнический
колледж» от 18.11.2022 № 01-01-06/567

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1С Колледж проф

г. Нефтеюганск
2022

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура – совокупность основных структурно-функциональных характеристик, свойств, компонентов 1С КОЛЛЕДЖА ПРОФ, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с 1С КОЛЛЕДЖЕМ ПРОФ и не включена оператором системы или сети в границу процесса оценки угроз безопасности информации.

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.

Возможности нарушителя – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

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

Информация – данные, содержащиеся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть (ИТКС) – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент – программное, программно-аппаратное или техническое средство, входящее в состав 1С КОЛЛЕДЖА ПРОФ.

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

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.

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.

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

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

Побочные электромагнитные излучения и наводки (ПЭМИН) – 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.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

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

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.

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

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

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

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

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

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

Угроза безопасности информации (УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

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

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Введение

2.1.1. Настоящая модель угроз безопасности информации (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.

2.1.2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в 1С Колледже проф (далее – 1С КОЛЛЕДЖ ПРОФ) (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в 1С КОЛЛЕДЖЕМ ПРОФ информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования 1С КОЛЛЕДЖА ПРОФ – актуальных угроз безопасности информации.

2.1.3. В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» настоящая Модель угроз подлежит использованию при формировании требований к системе защиты ПДн, обрабатываемых в 1С КОЛЛЕДЖЕ ПРОФ.

2.2. Источники разработки

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

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

– в случае определения АУ «Нефтеюганский политехнический колледж» (далее – АУ «Нефтеюганский политехнический колледж») необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.

2.2.2. Перечень нормативных правовых актов, методических документов и национальных стандартов, используемый для оценки угроз безопасности информации и разработки Модели угроз, представлен в Приложении № 1.

2.3. Оцениваемые угрозы

2.3.1. Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (далее – ТКУИ), по причинам, перечисленным в таблице 1.

Таблица 1 – Обоснования исключения угроз, реализуемых за счет ТКУИ

№ п/п	Угрозы, связанные с техническими каналами утечки информации	Обоснование исключения
1.	Угрозы утечки акустической (речевой) информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящую специализированную аппаратуру, регистрирующую акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки информации, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
2.	Угрозы утечки видовой информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих специализированные оптические (оптико-электронные) средства для просмотра информации с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
3.	Угрозы утечки информации по каналам ПЭМИН	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящие специализированные технические средства перехвата побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз

* За исключением угроз, характеризующихся использованием нарушителями портативных (мобильных) устройств съема информации (планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

2.4. Ответственность за обеспечение защиты информации (безопасности)

2.4.1. Ответственными за обеспечение безопасности ПДн при их обработке в 1С КОЛЛЕДЖЕ ПРОФ приказом Директора АУ «Нефтеюганский политехнический колледж» назначены должностные лица / подразделения, представленные в таблице 2.

Таблица 2 – Ответственные за обеспечение защиты информации (безопасности)

№ п/п	Роль подразделения / должностного лица	Должностное лицо / подразделение
1.	Ответственный за обеспечение безопасности персональных данных	заведующий отделом информационных технологий

2.5. Особенности пересмотра Модели угроз

2.5.1. Настоящая Модель угроз может быть пересмотрена:

– по решению АУ «Нефтеюганский политехнический колледж» на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений 1С КОЛЛЕДЖА ПРОФ;

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

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования 1С КОЛЛЕДЖА ПРОФ;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в 1С КОЛЛЕДЖЕ ПРОФ и (или) взаимодействующих (смежных) системах.

3. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

3.1. Общее описание объекта оценки угроз

3.1.1. Настоящая Модель угроз разработана в отношении 1С КОЛЛЕДЖА ПРОФ.

3.1.2. Основные характеристики 1С КОЛЛЕДЖА ПРОФ:

3.1.3. Состав обрабатываемой информации:

– Персональные данные.

3.1.4. Основные процессы (бизнес-процессы), для обеспечения которых создана 1С КОЛЛЕДЖ ПРОФ:

– Осуществление образовательной деятельности (Предполагает организацию и ведение образовательной деятельности в соответствии с законодательством).

3.1.5. Уровень защищенности ПДн: 4

3.2. Состав и архитектура объекта оценки

3.2.1. Состав 1С КОЛЛЕДЖА ПРОФ определен в таблице 3.

Таблица 3 – Состав 1С КОЛЛЕДЖА ПРОФ

№ п/п	Характеристика	Значение характеристики
1.	Программно-аппаратные средства	Отдел кадров ПК1 – 1 Отдел кадров ПК 2 – 1 Бухгалтерия ПК 1 – 1 Бухгалтерия ПК 2 – 1 Бухгалтерия ПК 3 – 1 Бухгалтерия ПК 4 – 1 Бухгалтерия ПК 5 – 1 Сервер DNS – 1 Контроллер домена – 2 Сервер SQL – 1 файловый сервер – 1 Сервер 1с – 2
2.	Общесистемное программное обеспечение	Операционные системы: - Debian GNU/Linux; - Microsoft Windows Server 2019 Standart, русская версия; - Microsoft Windows Server 2012 R2 Standart x64; - Microsoft Windows 10 Pro, 64-разрядная
3.	Прикладное программное обеспечение	- 1С Электронное обучение; - 1С Колледж ПРоф
4.	Средства защиты информации	**Средства антивирусной защиты:** - Kaspersky Endpoint Security для Windows (версия 11.1.1.126) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2024) **Средства криптографической защиты информации:** - Программный комплекс ViPNet Client 4 (версия 4.5) (исполнение 2) (Сертифицирующий орган ФСБ России

№ п/п	Характеристика	Значение характеристики
		№ СФ/124-4062 от 18.05.2021 действителен до 18.05.2024)

3.2.2. 1С КОЛЛЕДЖ ПРОФ представляет собой локальную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в пределах одного здания (нескольких близко расположенных зданий) и объединенных в единую систему) со следующими характеристиками:

3.2.2.1. Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – присутствует, в соответствии с таблицей 4.

Таблица 4 – Подключения к сетям 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, беспроводной, протоколы TCP/IP, HTTP, POP3, FTP, SMTP, IMAP4
2.	общего пользования	ООО Интелком	оказание услуг	Тип доступа проводной, протоколы FTP, HTTP, IMAP4, POP3, SMTP, TCP/IP

3.2.2.2. Подключение к информационно-телекоммуникационным сетям АУ «Нефтеюганский политехнический колледж» – отсутствует.

3.2.2.3. Подключение к информационно-телекоммуникационной сети «Интернет» – отсутствует.

3.2.2.4. Подключение к информационно-телекоммуникационным сетям иных организаций – отсутствует.

3.2.2.5. В 1С КОЛЛЕДЖЕ ПРОФ не осуществляется взаимодействие с системами и сетями других организаций.

3.2.2.6. В 1С КОЛЛЕДЖЕ ПРОФ не осуществляется взаимодействие с другими системами и сетями АУ «Нефтеюганский политехнический колледж».

3.2.2.7. К информационным ресурсам 1С КОЛЛЕДЖА ПРОФ не осуществляется локальный доступ.

3.2.2.8. К информационным ресурсам 1С КОЛЛЕДЖА ПРОФ не осуществляется удаленный доступ.

3.2.3. Технологии, используемые в 1С КОЛЛЕДЖЕ ПРОФ отражены в таблице 5.

Таблица 5 – Технологии, используемые в 1С КОЛЛЕДЖЕ ПРОФ

№ п/п	Технология	Используется / Не используется
1.	Съемные носители информации	Не используются
2.	Технология виртуализации	Используются
3.	Технология беспроводного доступа	Не используются
4.	Мобильные технические средства	Не используются
5.	Веб-серверы	Используются
6.	Технология веб-доступа	Не используются
7.	Smart-карты	Не используются
8.	Технологии грид-систем	Не используются
9.	Технологии суперкомпьютерных систем	Не используются
10.	Большие данные	Не используются
11.	Числовое программное оборудование	Не используются
12.	Одноразовые пароли	Не используются
13.	Электронная почта	Не используется
14.	Технология передачи видеоинформации	Не используется
15.	Технология удаленного рабочего стола	Не используются
16.	Технология удаленного администрирования	Не используются
17.	Технология удаленного внеполосного доступа	Не используются
18.	Технология передачи речи	Не используются
19.	Технология искусственного интеллекта	Не используются

3.2.4. 1С КОЛЛЕДЖ ПРОФ функционирует на базе инфраструктуры АУ «Нефтеюганский политехнический колледж».

4. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

4.2. Негативные последствия определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивает 1С КОЛЛЕДЖ ПРОФ, и применительно к нарушению безопасности информации, содержащейся в 1С КОЛЛЕДЖЕ ПРОФ.

4.3. На основе анализа исходных данных 1С КОЛЛЕДЖА ПРОФ определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 6.

Таблица 6 – Виды рисков (ущерба) и негативные последствия

Идентификатор	Негативные последствия	Вид риска (ущерба)
НП.1	Разглашение персональных данных граждан	У1. Ущерб физическому лицу
НП.2	Нарушение неприкосновенности частной жизни	У1. Ущерб физическому лицу
НП.3	Нарушение личной, семейной тайны, утрата чести и доброго имени	У1. Ущерб физическому лицу
НП.4	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	У1. Ущерб физическому лицу
НП.5	Нарушение конфиденциальности (утечка) персональных данных	У1. Ущерб физическому лицу
НП.6	Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.7	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.8	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.9	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

Идентификатор	Негативные последствия	Вид риска (ущерба)
НП.10	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

5. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

5.1. В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты 1С КОЛЛЕДЖА ПРОФ, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, определенным в разделе 4 настоящей Модели угроз, – объектов воздействия.

5.2. Объекты воздействия определялись для реальной архитектуры и условий функционирования 1С КОЛЛЕДЖА ПРОФ на основе анализа исходных данных и проведенной инвентаризации.

5.3. Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

5.4. В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 7.

Таблица 7 – Виды воздействия

Идентификатор	Вид воздействия
ВВ.1	утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач
ВВ.6	нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

5.5. Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 8.

Таблица 8 – Объекты воздействия и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
Нарушение неприкосновенности частной жизни	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение личной, семейной тайны, утрата чести и доброго имени	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
Нарушение конфиденциальности (утечка) персональных данных	Веб-сайт	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутиза-	ВВ.2; ВВ.3; ВВ.4; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	торы, коммутаторы, IoT-устройства и т.п.)	
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	BIOS/UEFI	ВВ.2; ВВ.3; ВВ.4
	Веб-сайт	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	XML-схема, передаваемая между клиентом и сервером	ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Веб-сервер	ВВ.2; ВВ.3; ВВ.4
	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4

Негативные последствия	Объекты воздействия	Виды воздействия
	Микропрограммное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое оборудование	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Система поддержания температурно-влажностного режима	ВВ.2; ВВ.3; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	BIOS/UEFI	ВВ.2; ВВ.3; ВВ.4
	Веб-сайт	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	XML-схема, передаваемая между клиентом и сервером	ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Веб-сервер	ВВ.2; ВВ.3; ВВ.4
	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Микропрограммное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое оборудование	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Система поддержания температурно-влажностного режима	ВВ.2; ВВ.3; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутиза-	ВВ.2; ВВ.3; ВВ.4; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	торы, коммутаторы, IoT-устройства и т.п.)	
Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4

6. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. Антропогенные источники

6.1.1. В ходе оценки угроз безопасности информации определяются возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие(ая) реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты 1С КОЛЛЕДЖА ПРОФ, – актуальные нарушители.

6.1.2. Процесс определения актуальных нарушителей включал:

6.1.2.1. Формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предположений об их отнесении к числу возможных нарушителей (нарушителей, подлежащих дальнейшей оценке), представленных в таблице 9.

Таблица 9 – Перечень рассматриваемых нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
1.	Специальные службы иностранных государств	Нанесение ущерба государству в области обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций; Получение конкурентных преимуществ на уровне государства; Срыв заключения международных договоров; Создание внутриполитического кризиса	Цели не предполагают потенциальное наличие нарушителя
2.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций	Цели не предполагают потенциальное наличие нарушителя
3.	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды; Желание самореализации (подтверждение статуса)	Цели не предполагают потенциальное наличие нарушителя
4.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды;	Возможные цели реализации угроз безопасности информации

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
		Любопытство или желание самореализации (подтверждение статуса)	предполагают наличие нарушителя
5.	Конкурирующие организации	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ	Цели не предполагают потенциальное наличие нарушителя
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия	Цели не предполагают потенциальное наличие нарушителя
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
8.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
10.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
11.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса);	Возможные цели реализации угроз безопасности информации

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
		Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	предполагают наличие нарушителя
12.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
13.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

6.1.2.2. Определение характеристик (категория нарушителя и уровень возможности по реализации угроз безопасности информации) возможных нарушителей.

6.1.2.3. Оценка возможности привлечения (вхождения в сговор) одними нарушителями других (в том числе обладающих привилегированными правами доступа).

6.1.2.4. Сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации. По результатам сопоставления определяются актуальные нарушители по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для 1С КОЛЛЕДЖА ПРОФ негативным последствиям и соответствующим рискам (видам ущерба).

6.1.3. Итоговые характеристики возможных нарушителей представлены в таблице 10.

Таблица 10 – Характеристики возможных нарушителей

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1.	Отдельные физические лица (хакеры)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
3.	Поставщики вычислительных услуг, услуг связи	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
6.	Авторизованные пользователи систем и сетей	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
7.	Системные администраторы и администраторы безопасности	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
8.	Бывшие (уволенные) работники (пользователи)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да

6.1.4. Категория нарушителя определяется исходя из следующих принципов:

– внешний нарушитель – если нарушитель не имеет прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам 1С КОЛЛЕДЖА ПРОФ, требующим авторизации;

– внутренний нарушитель – если нарушитель имеет права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам 1С КОЛЛЕДЖА ПРОФ. К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам 1С КОЛЛЕДЖА ПРОФ.

6.1.5. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

6.1.6. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителя по реализации угроз безопасности информации.

6.1.7. Уровень возможности нарушителя определяется исходя из следующих принципов:

– нарушитель, обладающий базовыми возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов;

– нарушитель, обладающий базовыми повышенными возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий средними возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе на выявленные им неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий высокими возможностями по реализации угроз безопасности информации – если имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.

6.1.8. Подробное описание уровней возможностей нарушителей по реализации угроз безопасности информации приведено в Приложении № 3.

7. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

7.1. В ходе оценки угроз безопасности информации определяются возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в 1С КОЛЛЕДЖЕ ПРОФ, – актуальные способы реализации (возникновения) угроз безопасности информации.

7.2. Процесс определения актуальных способов реализации (возникновения) угроз безопасности информации включал:

7.2.1. Составление перечня рассматриваемых (возможных) способов реализации угроз безопасности. Перечень возможных способов реализации угроз безопасности информации представлен в таблице 11.

Таблица 11 – Перечень возможных способов реализации угроз безопасности информации

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного программного обеспечения
СР.3	Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
СР.4	Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
СР.6	Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.8	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.9	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств
СР.10	Перехват трафика сети передачи данных
СР.11	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
СР.12	Реализация атак типа "отказ в обслуживании" в отношении технических средств, программного обеспечения и каналов передачи данных

7.2.2. Определение интерфейсов объектов воздействия, определенных в соответствии с разделом 5 настоящей Модели угроз. Интерфейсы объектов воздействия определялись на основе изучения и анализа данных:

– об архитектуре, составе и условиях функционирования 1С КОЛЛЕДЖА ПРОФ;

– о группах пользователей 1С КОЛЛЕДЖА ПРОФ, их типов доступа и уровней полномочий.

7.2.3. Определение наличия у актуальных нарушителей возможности доступа к интерфейсам объектов воздействия.

7.2.4. Определение актуальных способов реализации (возникновения) угроз безопасности информации актуальным нарушителем через доступные ему интерфейсы объектов воздействия.

7.3. Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации, включающие описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям, представлены в таблице 12.

Таблица 12 – Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Вид нарушителя	**Категория нарушителя**	**Объекты воздействия**	**Доступные интерфейсы**	**Способы реализации (идентификатор)**
Отдельные физические лица (хакеры)	Внешний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Информационная (автоматизированная) система	Пользователи	СР.1
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
		Защищаемая информация	Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
Поставщики вычислительных услуг, услуг связи	Внутренний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Веб-сайт	Веб-интерфейс системы администрирования Веб-сайта	СР.9
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Веб-сервер	Служебные программы командной строки для управления Веб-сервером	СР.8; СР.9
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Защищаемая информация	Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Информационная (автоматизированная) система	Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4
		Прикладное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Системное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Учетные данные пользователя	Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Защищаемая информация	Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Объекты файловой системы	Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
Авторизованные пользователи систем и сетей	Внутренний	BIOS/UEFI	Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
		Веб-сайт	Веб-интерфейс пользователя Веб-сайта	СР.1; СР.2
		XML-схема, передаваемая между клиентом и сервером	Каналы связи узлов локальной вычислительной сети	СР.10
		База данных	Прикладное приложение, использующее базу данных	СР.1
		Веб-сервер	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к виртуальным машинам	СР.1; СР.2
			Виртуальные каналы передачи данных	СР.10
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
			Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Системные администраторы и администраторы безопасности	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Веб-сайт	Веб-интерфейс системы администрирования Веб-сайта	СР.9
		XML-схема, передаваемая между клиентом и сервером	Каналы связи узлов локальной вычислительной сети	СР.10
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Веб-сервер	Служебные программы командной строки для управления Веб-сервером	СР.8; СР.9
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к виртуальным машинам	СР.1; СР.2
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		данных, систему управления виртуальной инфраструктурой)	Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Информационная (автоматизированная) система	Процесс создания (модернизации) информационной (автоматизированной) системы	СР.4; СР.8; СР.9
			Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Канал удаленного администрирования СКЗИ	СР.1
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Бывшие (уволенные) работники (пользователи)	Внешний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные ра-	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		бочие места, сервера, мар-шрутизаторы, коммутаторы, IoT-устройства и т.п.)		
		Учетные данные пользовате-ля	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

8. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

8.1. В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для 1С КОЛЛЕДЖА ПРОФ – актуальные угрозы безопасности информации.

8.2. Процесс определения актуальных угроз безопасности информации включал:

8.2.1. Выделение из исходного перечня угроз безопасности информации возможных угроз по следующему принципу: угроза безопасности информации признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

Перечень исключенных из исходного перечня угроз безопасности информации представлен в Приложении № 4.

8.2.2. Оценку возможных угроз на предмет актуальности по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

Сценарии определяются для соответствующих способов реализации угроз безопасности информации.

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации представлен в Приложении № 5.

8.3. По результатам оценки возможных угроз безопасности выявлено актуальных угроз: 133. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 13.

Таблица 13 – Актуальные угрозы безопасности информации

Идентификатор угрозы	**Наименование угрозы**
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации

Идентификатор угрозы	Наименование угрозы
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.033	Угроза использования слабостей кодирования входных данных
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.041	Угроза межсайтового скриптинга
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи

Идентификатор угрозы	Наименование угрозы
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.088	Угроза несанкционированного копирования защищаемой информации
УБИ.089	Угроза несанкционированного редактирования реестра
УБИ.090	Угроза несанкционированного создания учётной записи пользователя
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.103	Угроза определения типов объектов защиты
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.108	Угроза ошибки обновления гипервизора
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники

Идентификатор угрозы	Наименование угрозы
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.128	Угроза подмены доверенного пользователя
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.156	Угроза утраты носителей информации
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.158	Угроза форматирования носителей информации
УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.162	Угроза эксплуатации цифровой подписи программного кода
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.169	Угроза наличия механизмов разработчика
УБИ.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.172	Угроза распространения «почтовых червей»

Идентификатор угрозы	Наименование угрозы
УБИ.173	Угроза «спама» веб-сервера
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
УБИ.179	Угроза несанкционированной модификации защищаемой информации
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
УБИ.182	Угроза физического устаревания аппаратных компонентов
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза перехвата управления информационной системой
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

9. ОЦЕНКА УГРОЗ В СООТВЕТСТВИИ С МЕТОДИЧЕСКИМИ ДОКУМЕНТАМИ ФСБ РОССИИ

9.1. На основании исходных данных об объектах защиты (в соответствии с разделом 5 настоящей Модели угроз) и источниках атак (в соответствии с разделом 6.1 настоящей Модели угроз) 1С КОЛЛЕДЖА ПРОФ определены обобщенные возможности источников атак (таблица 14).

Таблица 14 – Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Предположение о возможности источников атак
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

9.2. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности информации определяется возможностями источников атак.

9.3. Исходя из обобщенных возможностей источников атак определены уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы). Результаты приведены в Приложении № 7.

9.4. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КС3.

Источники разработки модели угроз

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

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– 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 Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;

– 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;

– 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 29099-91 «Сети вычислительные локальные. Термины и определения», утвержденный постановлением Комитета стандартизации и метрологии СССР от 25 сентября 1991 г. № 1491;

– ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1520-ст;

– ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1521-ст;

– ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. № 3469;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», утвержденный постановлением Госстандарта России от 9 февраля 1995 г. № 49;

– 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 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», утвержденный постановлением Госстандарта России от 14 июля 1998 г. № 295;

– 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 2.105-2019 «Единая система конструкторской документации. Общие требования к текстовым документам», утвержденный приказом Росстандарта от 29 апреля 2019 г. № 175-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 Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов», утвержденный приказом Росстандарта от 25 октября 2021 г. № 1297-ст;

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

Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
1.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.5	НП.8; НП.9; НП.10	–
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	НП.5	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7	–
3.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	–	НП.10	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.8; НП.10	–
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	–	НП.10	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.8; НП.10	–
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.10	–
6.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.3; НП.5	НП.10	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.5	НП.6; НП.7; НП.10	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–
7.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.5	НП.10	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.5	НП.6; НП.7; НП.8; НП.10	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–
8.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–

Уровни возможностей нарушителя

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
Н1	Нарушитель, обладающий базовыми возможностями	– Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. – Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. – Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним
Н2	Нарушитель, обладающий базовыми повышенными возможностями	– Обладает всеми возможностями нарушителей с базовыми возможностями. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. – Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. – Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. – Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах
Н3	Нарушитель, обладающий средними возможностями	– Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. – Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств.

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
		– Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. – Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. – Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. – Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц
Н4	Нарушитель, обладающий высокими возможностями	– Обладает всеми возможностями нарушителей со средними возможностями. – Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». – Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. – Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. – Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. – Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. – Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. – Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей

Перечень исключенных из базового перечня угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Отсутствуют объекты воздействия
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Отсутствуют объекты воздействия
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Отсутствуют объекты воздействия
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Отсутствуют объекты воздействия
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Отсутствуют объекты воздействия
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Отсутствуют объекты воздействия
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.026	Угроза искажения XML-схемы	Отсутствуют условия, при которых может быть реализована угроза
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Отсутствуют объекты воздействия
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.040	Угроза конфликта юрисдикций различных стран	Отсутствуют объекты воздействия
УБИ.042	Угроза межсайтовой подделки запроса	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.043	Угроза нарушения доступности облачного сервера	Отсутствуют объекты воздействия
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Отсутствуют объекты воздействия
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Отсутствуют объекты воздействия
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Отсутствуют объекты воздействия
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Отсутствуют объекты воздействия
УБИ.055	Угроза незащищённого администрирования облачных услуг	Отсутствуют объекты воздействия
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Отсутствуют объекты воздействия
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Отсутствуют объекты воздействия
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Отсутствуют объекты воздействия
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Отсутствуют объекты воздействия
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Отсутствуют объекты воздействия
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Отсутствуют объекты воздействия
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Отсутствуют объекты воздействия
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Отсутствуют объекты воздействия
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Отсутствуют объекты воздействия
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.097	Угроза несогласованности правил доступа к большим данным	Отсутствуют объекты воздействия
УБИ.101	Угроза общедоступности облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Отсутствуют объекты воздействия
УБИ.107	Угроза отключения контрольных датчиков	Отсутствуют объекты воздействия
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Отсутствуют объекты воздействия
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Отсутствуют объекты воздействия
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Отсутствуют объекты воздействия
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Отсутствуют объекты воздействия
УБИ.127	Угроза подмены действия пользователя путём обмана	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.131	Угроза подмены субъекта сетевого доступа	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.132	Угроза получения предварительной информации об объекте защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Отсутствуют объекты воздействия
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Отсутствуют условия, при которых может быть реализована угроза
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.137	Угроза потери управления облачными ресурсами	Отсутствуют объекты воздействия
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Отсутствуют объекты воздействия
УБИ.139	Угроза преодоления физической защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.141	Угроза привязки к поставщику облачных услуг	Отсутствуют объекты воздействия
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Отсутствуют объекты воздействия
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Отсутствуют объекты воздействия
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Отсутствуют объекты воздействия
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Отсутствуют объекты воздействия
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Отсутствуют объекты воздействия
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Отсутствуют объекты воздействия
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Отсутствуют объекты воздействия
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Отсутствуют объекты воздействия
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.189	Угроза маскирования действий вредоносного кода	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Отсутствуют объекты воздействия
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Отсутствуют объекты воздействия
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Отсутствуют объекты воздействия
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Отсутствуют объекты воздействия
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Отсутствуют объекты воздействия
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Отсутствуют объекты воздействия
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.213	Угроза обхода многофакторной аутентификации	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Отсутствуют объекты воздействия
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Отсутствуют объекты воздействия
УБИ.219	Угроза хищения обучающих данных	Отсутствуют объекты воздействия
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Отсутствуют объекты воздействия
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Отсутствуют объекты воздействия
УБИ.222	Угроза подмены модели машинного обучения	Отсутствуют объекты воздействия

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях	Т1.1 Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2 Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.3 Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4 Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.5 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств
		Т1.6 Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора
		Т1.7 Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		Т1.8 Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.9 Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.
		Т1.10 Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)

№	Тактика	Основные техники
		T1.11 Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		T1.12 Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		T1.13 Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		T1.14 Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		T1.15 Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
		T1.16 Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров
		T1.17 Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.18 Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.19 Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.20 Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.21 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем анализа и обобщения информации перехватываемой в сети передачи информации

№	Тактика	Основные техники
		Т1.22 Поиск и покупка специализированного программного обеспечения (вредоносного кода) на специализированных нелегальных площадках
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1 Использование внешних сервисов организации в сетях публичного доступа (Интернет)
		Т2.2 Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра
		Т2.3 Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.4 Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.5 Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке
		Т2.6 Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
		Т2.7 Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций
		Т2.8 Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.9 Несанкционированное подключение внешних устройств
		Т2.10 Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
		Т2.11 Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
		Т2.12 Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа
		Т2.13 Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки
		Т2.14 Доступ путем эксплуатации недостатков систем биометрической аутентификации

№	Тактика	Основные техники
		Т2.15 Доступ путем использования недостатков правовых норм других стран, участвующих в трансграничной передаче облачного трафика
		Т2.16 Доступ путем использования возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1 Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.2 Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
		Т3.3 Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
		Т3.4 Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
		Т3.5 Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
		Т3.6 Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
		Т3.7 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т3.8 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т3.9 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т3.10 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т3.11 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «даркнет») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами

№	Тактика	Основные техники
		Т3.12 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.13 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.14 Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		Т3.15 Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
		Т3.16 Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL
		Т3.17 Планирование запуска вредоносного кода при запуске компьютера путем эксплуатации стандартных механизмов BIOS (UEFI) и т.п.
		Т3.18 Эксплуатация уязвимостей типа локальное исполнение программного кода
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1 Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2 Использование штатных средств удаленного доступа и управления операционной системы
		Т4.3 Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода
		Т4.4 Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
		Т4.5 Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети

№	Тактика	Основные техники
		Т4.6 Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
		Т4.7 Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей
		Т4.8 Использование прошивок устройств с уязвимостями, к примеру, внедрение новых функций в BIOS (UEFI)
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1 Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		Т5.2 Использование штатных средств удаленного доступа и управления операционной системы
		Т5.3 Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т5.4 Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т5.5 Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т5.6 Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения
		Т5.7 Туннелирование трафика управления через VPN
		Т5.8 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т5.9 Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
		Т5.10 Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
		Т5.11 Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		Т5.12 Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.

№	Тактика	Основные техники
		Т5.13 Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения
Т6	Повышение привилегий по доступу к компонентам систем и сетей	Т6.1 Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
		Т6.2 Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий
		Т6.4 Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи)
		Т6.5 Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций
		Т6.6 Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима
		Т6.7 Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями
		Т6.8 Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей
		Т6.9 Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1 Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения
		Т7.2 Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3 Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4 Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов

№	Тактика	Основные техники
		Т7.5 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
		Т7.6 Подделка данных вывода средств защиты от угроз информационной безопасности
		Т7.7 Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
		Т7.8 Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки
		Т7.9 Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей
		Т7.10 Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
		Т7.11 Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе
		Т7.12 Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности
		Т7.13 Создание скрытых файлов, скрытых учетных записей
		Т7.14 Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
		Т7.15 Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
		Т7.16 Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки
		Т7.17 Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети

№	Тактика	Основные техники
		Т7.18 Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе
		Т7.19 Туннелирование трафика управления через VPN
		Т7.20 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т7.21 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22 Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т7.24 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т7.25 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т7.26 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т7.27 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т7.29 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы

№	Тактика	Основные техники
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1 Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
		Т8.2 Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
		Т8.3 Использование механизмов дистанционной установки программного обеспечения и конфигурирования
		Т8.4 Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям
		Т8.5 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т8.6 Копирование вредоносного кода на съемные носители
		Т8.7 Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
		Т8.8 Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1 Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		Т9.2 Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		Т9.3 Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т9.4 Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т9.5 Отправка данных по известным протоколам управления и передачи данных
		Т9.6 Отправка данных по собственным протоколам
		Т9.7 Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения
		Т9.8 Туннелирование трафика передачи данных через VPN
		Т9.9 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие

№	Тактика	Основные техники
		Т9.10 Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т9.11 Отправка данных через альтернативную среду передачи данных
		Т9.12 Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации
		Т9.13 Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
		Т9.14 Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1 Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		Т10.2 Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		Т10.3 Несанкционированное воздействие на программные модули прикладного программного обеспечения
		Т10.4 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
		Т10.5 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения
		Т10.6 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства
		Т10.7 Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
		Т10.8 Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
		Т10.9 Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.10 Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
		Т10.11 Нецелевое использование ресурсов системы
		Т10.12 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов,

№	Тактика	Основные техники
		объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.13 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.14 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.15 Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой

Результаты оценки возможных угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средства криптографической защиты информации	НП.5; НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.003: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т10 (Т10.2; Т10.5)
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.9; СР.11	Сценарий реализации УБИ.004: – Т1 (Т1.9; Т1.15; Т1.16); – Т2 (Т2.9)
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.006: – Т1 (Т1.4; Т1.5); – Т2 (Т2.5; Т2.10); – Т3 (Т3.1; Т3.2; Т3.15); – Т4 (Т4.2); – Т5 (Т5.2)
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.3; СР.9	Сценарий реализации УБИ.007: – Т1 (Т1.9; Т1.16); – Т2 (Т2.6); – Т3 (Т3.5); – Т6 (Т6.2; Т6.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.008: – Т1 (Т1.6); – Т2 (Т2.10); – Т4 (Т4.1)
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.8; СР.9	Сценарий реализации УБИ.009: – Т1 (Т1.9); – Т3 (Т3.18); – Т4 (Т4.8)
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.2	Сценарий реализации УБИ.010: – Т1 (Т1.5; Т1.9; Т1.16; Т1.22); – Т2 (Т2.5; Т2.6); – Т3 (Т3.1; Т3.2)
УБИ.012	Угроза деструктивного	Внутренний нарушитель, обладающий базовыми возможностями,	Микропрограммное обеспечение, Объек-	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.3; СР.9	Сценарий реализации УБИ.012: – Т1 (Т1.9; Т1.16);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	изменения конфигурации/среды окружения программ	Внутренний нарушитель, обладающий базовыми повышенными возможностями	ты файловой системы, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение			– Т2 (Т2.5; Т2.6); – Т3 (Т3.7)
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.013: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.3; СР.9	Сценарий реализации УБИ.014: – Т1 (Т1.5; Т1.16; Т1.19); – Т2 (Т2.5; Т2.6)
УБИ.015	Угроза доступа к защищаемым	Внешний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	НП.5; НП.8; НП.9; НП.10	СР.1; СР.3	Сценарий реализации УБИ.015:

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	файлам с использованием обходного пути	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				– Т1 (Т1.9; Т1.16); – Т2 (Т2.3; Т2.5; Т2.6); – Т6 (Т6.3; Т6.6)
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.018: – Т2 (Т2.5); – Т10 (Т10.2)
УБИ.019	Угроза заражения DNS-кеша	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.019: – Т8 (Т8.8)
УБИ.022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение	НП.8; НП.9	СР.2; СР.4	Сценарий реализации УБИ.022: – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.2; Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.4	Сценарий реализации УБИ.023: – Т2 (Т2.7); – Т3 (Т3.7); – Т10 (Т10.3)
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.3	Сценарий реализации УБИ.025: – Т10 (Т10.2; Т10.4)
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2; СР.3	Сценарий реализации УБИ.027: – Т3 (Т3.2); – Т8 (Т8.1)
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.028: – Т1 (Т1.5; Т1.9); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.030: – Т1 (Т1.1; Т1.9; Т1.16); – Т2 (Т2.4)
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.8	Сценарий реализации УБИ.031: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.4; Т2.5); – Т6 (Т6.3; Т6.6)
УБИ.033	Угроза использования слабостей кодирования входных данных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.033: – Т1 (Т1.5); – Т2 (Т2.5; Т2.6); – Т10 (Т10.2)
УБИ.034	Угроза использования слабостей про-	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Сетевое программное обеспечение, Сетевой трафик, Системное	НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.3	Сценарий реализации УБИ.034: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	токолов сетевого/локального обмена данными	Внутренний нарушитель, обладающий базовыми повышенными возможностями	программное обеспечение			– Т10 (Т10.1)
УБИ.036	Угроза исследования механизмов работы программы	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.8	Сценарий реализации УБИ.036: – Т2 (Т2.5)
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.037: – Т1 (Т1.9); – Т2 (Т2.5; Т2.6)
УБИ.041	Угроза межсайтового скриптинга	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.041: – Т1 (Т1.1; Т1.5; Т1.8); – Т2 (Т2.1); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.2	Сценарий реализации УБИ.044: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.3; Т2.5); – Т3 (Т3.1); – Т10 (Т10.2; Т10.3)
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1	Сценарий реализации УБИ.045: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6); – Т10 (Т10.2; Т10.6)
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.046: – Т2 (Т2.4; Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.048: – Т2 (Т2.3; Т2.5); – Т3 (Т3.7); – Т4 (Т4.3; Т4.5; Т4.7); – Т10 (Т10.2; Т10.7)
УБИ.049	Угроза нарушения целостности данных кеша	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.049: – Т2 (Т2.5); – Т3 (Т3.9); – Т10 (Т10.1; Т10.2)
УБИ.051	Угроза невозможности восстановления	Внутренний нарушитель, обладающий базовыми возможностями,	Узел вычислительной сети (автоматизиро-	НП.1; НП.5; НП.8; НП.9; НП.10	СР.9	Сценарий реализации УБИ.051: – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель, обладающий базовыми повышенными возможностями	ванные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.11	Сценарий реализации УБИ.053: – Т2 (Т2.5)
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.8; СР.9	Сценарий реализации УБИ.059: – Т10 (Т10.10)
УБИ.061	Угроза некорректного за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	База данных, Сетевое программное обеспечение, Сетевой трафик	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.061: – Т1 (Т1.5); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	дания структуры данных транзакции					
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение	НП.8; НП.9	СР.1; СР.2; СР.9	Сценарий реализации УБИ.062: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.063: – Т2 (Т2.5); – Т10 (Т10.11)
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.7; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.067: – Т1 (Т1.13; Т1.14); – Т10 (Т10.1)
УБИ.068	Угроза неправомерного/некорректного использования интерфейса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.068: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	взаимодействия с приложением		программное обеспечение, Системное программное обеспечение			
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.069: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.071: – Т1 (Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.072: – Т2 (Т2.5); – Т3 (Т3.8; Т3.18); – Т4 (Т4.6)
УБИ.073	Угроза несанкционированного доступа к активному и	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-	НП.8; НП.9	СР.1; СР.2; СР.9	Сценарий реализации УБИ.073: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	(или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети		шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой), Микропрограммное обеспечение, Сетевое оборудование, Сетевое программное обеспечение			
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.074: – Т1 (Т1.12); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.075	Угроза несанкционированного доступа к виртуальным	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.075: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	каналам передачи	Внутренний нарушитель, обладающий базовыми повышенными возможностями	шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.076: – Т10 (Т10.10)
УБИ.077	Угроза несанкционированного доступа к данным за пределами за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы вирту-	НП.8; НП.9	СР.1; СР.2	Сценарий реализации УБИ.077: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.1); – Т4 (Т4.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	резервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение		альных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			– Т7 (Т7.18); – Т10 (Т10.1; Т10.11)
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.8; СР.9	Сценарий реализации УБИ.078: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства,	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.079: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	стороны других виртуальных машин		виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.080: – Т1 (Т1.5; Т1.16); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.084: – Т1 (Т1.5; Т1.22)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.7; НП.10	СР.1; СР.8	Сценарий реализации УБИ.085: – Т1 (Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Учетные данные пользователя	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.086: – Т1 (Т1.5; Т1.12; Т1.22); – Т2 (Т2.4; Т2.11); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.087: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.088: – Т2 (Т2.4; Т2.9); – Т10 (Т10.1)
УБИ.089	Угроза несанкционированного редактирования реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.089: – Т1 (Т1.5; Т1.9); – Т2 (Т2.4); – Т4 (Т4.5); – Т10 (Т10.1)
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.090: – Т1 (Т1.5); – Т2 (Т2.4); – Т4 (Т4.1); – Т5 (Т5.2); – Т10 (Т10.2)
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.091: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.093: – Т1 (Т1.9); – Т2 (Т2.4; Т2.5); – Т3 (Т3.2); – Т10 (Т10.1)
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.094: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1; Т10.3)
УБИ.095	Угроза несанкционированного управления указателями	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.095: – Т1 (Т1.5); – Т2 (Т2.4; Т2.11); – Т3 (Т3.2); – Т10 (Т10.3; Т10.4)
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы,	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.098: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			коммутаторы, IoT-устройства и т.п.)			
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.099: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.8; СР.9	Сценарий реализации УБИ.100: – Т2 (Т2.4; Т2.5); – Т4 (Т4.1); – Т6 (Т6.6)
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.102: – Т2 (Т2.5)
УБИ.103	Угроза определения типов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.8; СР.9	Сценарий реализации УБИ.103: – Т1 (Т1.1; Т1.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	объектов защиты		трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			– Т2 (Т2.4)
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.104: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3)
УБИ.108	Угроза ошибки обновления гипервизора	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.108: – Т2 (Т2.5); – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			инфраструктурой)			
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.109: – Т2 (Т2.5; Т2.6); – Т10 (Т10.10)
УБИ.111	Угроза передачи данных по скрытым каналам	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик, Системное программное обеспечение	НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.111: – Т2 (Т2.4); – Т9 (Т9.10)
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.113: – Т2 (Т2.5; Т2.11); – Т10 (Т10.8)
УБИ.114	Угроза переполнения целочисленных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.114: – Т1 (Т1.1; Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.115	Угроза перехвата вводимой	Внешний нарушитель, обладающий базовыми возможностями,	Прикладное программное обеспечение,	НП.1; НП.5; НП.8; НП.9;	СР.1; СР.2	Сценарий реализации УБИ.115:

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.10		– Т1 (Т1.4; Т1.12); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т10 (Т10.1; Т10.3)
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.116: – Т1 (Т1.3); – Т2 (Т2.4; Т2.5; Т2.11)
УБИ.117	Угроза перехвата привилегированного потока	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.117: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т6 (Т6.1); – Т10 (Т10.1)
УБИ.118	Угроза перехвата привилегированного процесса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.118: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т6 (Т6.3)
УБИ.119	Угроза перехвата управления гипервизором	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.119: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.120	Угроза перехвата управления средой виртуализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.120: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)
УБИ.121	Угроза повреждения системного реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.121: – Т2 (Т2.4; Т2.5; Т2.11); – Т10 (Т10.8; Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
		Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.122	Угроза повышения привилегий	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение	НП.8; НП.9	СР.1; СР.2; СР.8	Сценарий реализации УБИ.122: – Т2 (Т2.5); – Т3 (Т3.5); – Т6 (Т6.1); – Т10 (Т10.3)
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.123: – Т1 (Т1.6); – Т2 (Т2.5; Т2.10); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.124: – Т1 (Т1.22); – Т2 (Т2.5; Т2.11); – Т7 (Т7.6)
УБИ.128	Угроза подмены доверенного пользователя	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.128: – Т1 (Т1.5); – Т2 (Т2.5; Т2.9)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.129: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.7); – Т4 (Т4.6; Т4.7)
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Сетевой трафик	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.130: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.2)
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9; СР.12	Сценарий реализации УБИ.140: – Т2 (Т2.3; Т2.5); – Т10 (Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Микропрограммное обеспечение, Сетевое оборудование	НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.143: – Т1 (Т1.5); – Т2 (Т2.5); – Т7 (Т7.8); – Т10 (Т10.10)
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1	Сценарий реализации УБИ.144: – Т1 (Т1.9; Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.6)
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.145: – Т2 (Т2.4; Т2.5; Т2.8); – Т3 (Т3.3)
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Системное программное обеспечение	НП.5; НП.8; НП.9; НП.10	СР.1; СР.4	Сценарий реализации УБИ.149: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.9	Сценарий реализации УБИ.150: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Внешний нарушитель, обладающий базовыми возможностями	Веб-сервер	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.151: – Т1 (Т1.5; Т1.22); – Т2 (Т2.3; Т2.5)
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.152: – Т1 (Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.10)
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.153: – Т1 (Т1.2; Т1.22); – Т2 (Т2.3; Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.154: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.8); – Т4 (Т4.6); – Т7 (Т7.22); – Т10 (Т10.6; Т10.10)
УБИ.155	Угроза утраты вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.155: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5; Т2.11); – Т10 (Т10.10)
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8; СР.9	Сценарий реализации УБИ.156: – Т1 (Т1.10); – Т10 (Т10.1; Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.9; СР.11	Сценарий реализации УБИ.157: – Т2 (Т2.2); – Т10 (Т10.8; Т10.10)
УБИ.158	Угроза форматирования носителей информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.158: – Т2 (Т2.2; Т2.5); – Т10 (Т10.8)
УБИ.159	Угроза «форсированного веб-браузинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.159: – Т2 (Т2.1; Т2.5); – Т10 (Т10.1)
УБИ.160	Угроза хищения средств хранения, обработки и (или)	Внешний нарушитель, обладающий базовыми возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое	НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.160: – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ввода/вывода/передачи информации		оборудование, Средство вычислительной техники			
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.4	Сценарий реализации УБИ.162: – Т1 (Т1.10); – Т3 (Т3.11; Т3.16)
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.163: – Т1 (Т1.3); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6; НП.8; НП.9	СР.9	Сценарий реализации УБИ.165: – Т2 (Т2.5)
УБИ.166	Угроза внедрения системной избыточности	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6; НП.8; НП.9	СР.9	Сценарий реализации УБИ.166: – Т2 (Т2.5)
УБИ.167	Угроза заражения компьюте-	Внутренний нарушитель, обладающий базовыми возможностями,	Узел вычислительной сети (автоматизированные рабочие мес-	НП.1; НП.5; НП.8; НП.9; НП.10	СР.2; СР.8	Сценарий реализации УБИ.167: – Т2 (Т2.4); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ра при посещении неблагонадёжных сайтов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	та, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Учетные данные пользователя	НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.168: – Т4 (Т4.1)
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.169: – Т2 (Т2.5; Т2.6); – Т3 (Т3.12)
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель, обладающий базовыми возможностями	Объекты файловой системы	НП.5; НП.8; НП.9; НП.10	СР.4	Сценарий реализации УБИ.170: – Т2 (Т2.4); – Т3 (Т3.3); – Т10 (Т10.8)
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, обладающий базовыми возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8; НП.9; НП.10	СР.2; СР.8	Сценарий реализации УБИ.171: – Т1 (Т1.2); – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.1); – Т4 (Т4.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.172	Угроза распространения «почтовых червей»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение	НП.8; НП.9	СР.1; СР.2; СР.8	Сценарий реализации УБИ.172: – Т1 (Т1.1); – Т2 (Т2.3)
УБИ.173	Угроза «спама» веб-сервера	Внешний нарушитель, обладающий базовыми возможностями	Веб-сервер	НП.8; НП.9	СР.1	Сценарий реализации УБИ.173: – Т1 (Т1.1); – Т2 (Т2.1)
УБИ.174	Угроза «фарминга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.174: – Т1 (Т1.1; Т1.8); – Т3 (Т3.3)
УБИ.175	Угроза «фишинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.175: – Т1 (Т1.1; Т1.11); – Т2 (Т2.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Внешний нарушитель, обладающий базовыми возможностями	Средство защиты информации	НП.8; НП.9	СР.1; СР.8; СР.12	Сценарий реализации УБИ.176: – Т10 (Т10.3; Т10.10)
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.177: – Т10 (Т10.14)
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.8; НП.9	СР.1; СР.3	Сценарий реализации УБИ.178: – Т2 (Т2.4; Т2.5); – Т10 (Т10.5)
УБИ.179	Угроза несанкционированной модифи-	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	НП.5; НП.8; НП.9; НП.10	СР.8; СР.11	Сценарий реализации УБИ.179: – Т2 (Т2.5); – Т10 (Т10.7; Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	кации защищаемой информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Система поддержания температурно-влажностного режима	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.180: – Т10 (Т10.14)
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.182: – Т10 (Т10.8; Т10.10)
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.185: – Т2 (Т2.4); – Т7 (Т7.4)
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение	НП.8; НП.9	СР.1; СР.2; СР.8	Сценарий реализации УБИ.186: – Т1 (Т1.1); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации	НП.8; НП.9	СР.1; СР.8; СР.9	Сценарий реализации УБИ.187: – Т2 (Т2.4); – Т7 (Т7.4); – Т10 (Т10.2)
УБИ.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.2; СР.9	Сценарий реализации УБИ.188: – Т2 (Т2.7); – Т3 (Т3.7; Т3.8; Т3.10); – Т7 (Т7.24); – Т10 (Т10.7)
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.2; СР.8; СР.9	Сценарий реализации УБИ.191: – Т3 (Т3.2)
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.9	Сценарий реализации УБИ.192: – Т2 (Т2.5); – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.2; СР.8	Сценарий реализации УБИ.203: – Т2 (Т2.5); – Т3 (Т3.2); – Т6 (Т6.3); – Т9 (Т9.11)
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель, обладающий базовыми возможностями	Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1; СР.8	Сценарий реализации УБИ.205: – Т2 (Т2.4)
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.2; СР.8	Сценарий реализации УБИ.208: – Т10 (Т10.11)
УБИ.209	Угроза несанкционированного доступа к	Внешний нарушитель, обладающий базовыми возможностями,	Средство вычислительной техники	НП.5; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.209: – Т10 (Т10.1; Т10.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	защищаемой памяти ядра процессора	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.8; НП.9	СР.1; СР.9	Сценарий реализации УБИ.211: – Т10 (Т10.2)
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система, Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.5; НП.6; НП.8; НП.9; НП.10	СР.1	Сценарий реализации УБИ.212: – Т2 (Т2.4; Т2.5); – Т8 (Т8.1); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6; НП.8; НП.9	СР.1; СР.8	Сценарий реализации УБИ.214: – Т7 (Т7.4)
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8; НП.9; НП.10	СР.1; СР.2	Сценарий реализации УБИ.217: – Т3 (Т3.8); – Т7 (Т7.24)

Уточненные возможности нарушителей и направления атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование 1С КОЛЛЕДЖ ПРОФ, не имеют возможности находиться в помещениях, где расположена 1С КОЛЛЕДЖ ПРОФ, в отсутствие пользователей 1С КОЛЛЕДЖ ПРОФ; – Работа пользователей 1С КОЛЛЕДЖ ПРОФ регламентирована; – Ответственный за обеспечение безопасности ПДн, администраторы 1С КОЛЛЕДЖ ПРОФ назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств 1С КОЛЛЕДЖ ПРОФ, в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Проводится обучение пользователей 1С КОЛЛЕДЖ ПРОФ мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ	Да	– Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц; – Документация на СКЗИ не хранится у ответственного пользователя криптосредств в металлическом сейфе (шкафу); – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Нет	– Работа пользователей 1С КОЛЛЕДЖ ПРОФ регламентирована; – Проводится обучение пользователей 1С КОЛЛЕДЖ ПРОФ мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Сведения о физических мерах защиты объектов, в которых размещена 1С КОЛЛЕДЖ ПРОФ, доступны ограниченному кругу сотрудников
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Да	– Работа пользователей 1С КОЛЛЕДЖ ПРОФ регламентирована;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Ответственный за обеспечение безопасности ПДн, администраторы 1С КОЛЛЕДЖ ПРОФ назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств 1С КОЛЛЕДЖ ПРОФ, в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – Проводится обучение пользователей 1С КОЛЛЕДЖ ПРОФ мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Пользователи 1С КОЛЛЕДЖ ПРОФ имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн; – Программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по обеспечению безопасности персональных данных

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование 1С КОЛЛЕДЖ ПРОФ, не имеют возможности находиться в помещениях, где расположена 1С КОЛЛЕДЖ ПРОФ, в отсутствие пользователей 1С КОЛЛЕДЖ ПРОФ; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
2.2	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 действий	Да	– В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода; – Корпуса системных блоков не защищены от вскрытия (не опечатаны/не опломбированы)

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
3.1	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
3.2	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
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	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
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного 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

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	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

Утверждена приказом АУ
«Нефтеюганский политехнический
колледж» от 18.11.2022 № 01-01-06/567

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Информационная система персональных данных «Бухгалтерский и кадровый учет»

г. Нефтеюганск
2022

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура – совокупность основных структурно-функциональных характеристик, свойств, компонентов ИСПДна «Бухгалтерский и кадровый учет», воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с ИСПДном «Бухгалтерский и кадровый учет» и не включена оператором системы или сети в границу процесса оценки угроз безопасности информации.

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.

Возможности нарушителя – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

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

Информация – данные, содержащиеся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть (ИТКС) – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент – программное, программно-аппаратное или техническое средство, входящее в состав ИСПДна «Бухгалтерский и кадровый учет».

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

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.

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.

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

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

Побочные электромагнитные излучения и наводки (ПЭМИН) – 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.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

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

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.

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

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

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

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

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

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

Угроза безопасности информации (УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

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

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Введение

2.1.1. Настоящая модель угроз безопасности информации (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.

2.1.2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в информационной системе персональных данных «Бухгалтерский и кадровый учет» (далее – ИСПДн «Бухгалтерский и кадровый учет») (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в ИСПДном «Бухгалтерский и кадровый учет» информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования ИСПДна «Бухгалтерский и кадровый учет» – актуальных угроз безопасности информации.

2.1.3. В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» настоящая Модель угроз подлежит использованию при формировании требований к системе защиты ПДн, обрабатываемых в ИСПДне «Бухгалтерский и кадровый учет».

2.2. Источники разработки

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

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

– в случае определения АУ «Нефтеюганский политехнический колледж» (далее – АУ «Нефтеюганский политехнический колледж») необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.

2.3. Оцениваемые угрозы

2.3.1. Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (далее – ТКУИ), по причинам, перечисленным в таблице 1.

Таблица 1 – Обоснования исключения угроз, реализуемых за счет ТКУИ

№ п/п	Угрозы, связанные с техническими каналами утечки информации	Обоснование исключения
1.	Угрозы утечки акустической (речевой) информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящую специализированную аппаратуру, регистрирующую акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки информации, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
2.	Угрозы утечки видовой информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих специализированные оптические (оптико-электронные) средства для просмотра информации с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
3.	Угрозы утечки информации по каналам ПЭМИН	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящие специализированные технические средства перехвата побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз

* За исключением угроз, характеризующихся использованием нарушителями портативных (мобильных) устройств съема информации (планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

2.4. Ответственность за обеспечение защиты информации (безопасности)

2.4.1. Ответственными за обеспечение безопасности ПДн при их обработке в ИСПДне «Бухгалтерский и кадровый учет» приказом Директора АУ «Нефтеюганский политехнический колледж» назначены должностные лица / подразделения, представленные в таблице 2.

Таблица 2 – Ответственные за обеспечение защиты информации (безопасности)

№ п/п	Роль подразделения / должностного лица	Должностное лицо / подразделение
1.	Ответственный за обеспечение безопасности персональных данных	заведующий отделом информационных технологий

2.5. Особенности пересмотра Модели угроз

2.5.1. Настоящая Модель угроз может быть пересмотрена:

– по решению АУ «Нефтеюганский политехнический колледж» на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений ИСПДна «Бухгалтерский и кадровый учет»;

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

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИСПДна «Бухгалтерский и кадровый учет»;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в ИСПДне «Бухгалтерский и кадровый учет» и (или) взаимодействующих (смежных) системах.

3. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

3.1. Общее описание объекта оценки угроз

3.1.1. Настоящая Модель угроз разработана в отношении ИСПДна «Бухгалтерский и кадровый учет».

3.1.2. Основные характеристики ИСПДна «Бухгалтерский и кадровый учет»:

3.1.3. Состав обрабатываемой информации:

– Персональные данные.

3.1.4. Основные процессы (бизнес-процессы), для обеспечения которых создана ИСПДн «Бухгалтерский и кадровый учет»:

– Управление персоналом и кадровый учет (Предполагает: подбор, адаптацию, оценку, обучение, развитие и мотивацию персонала; выполнение требований трудового законодательства Российской Федерации в части ведения кадрового, воинского учета; организацию постановки на персонифицированный учет в системе обязательного пенсионного страхования; формирование кадрового резерва);

– Бухгалтерский учет (Предполагает выполнение требований трудового законодательства Российской Федерации в части ведения бухгалтерского учета, осуществление расчета заработной платы и иных выплат и удержаний).

3.1.5. Уровень защищенности ПДн: 3.

3.2. Состав и архитектура объекта оценки

3.2.1. Состав ИСПДна «Бухгалтерский и кадровый учет» определен в таблице 3.

Таблица 3 – Состав ИСПДна «Бухгалтерский и кадровый учет»

№ п/п	Характеристика	Значение характеристики
1.	Программно-аппаратные средства	Отдел кадров ПК1 – 1 Отдел кадров ПК 2 – 1 Бухгалтерия ПК 1 – 1 Бухгалтерия ПК 2 – 1 Бухгалтерия ПК 3 – 1 Бухгалтерия ПК 4 – 1 Бухгалтерия ПК 5 – 1 Сервер 1с – 1 Контроллер домена – 2 Сервер SQL – 1 файловый сервер – 1
2.	Общесистемное программное обеспечение	Операционные системы: - Microsoft Windows Server 2019 Standart, русская версия; - Microsoft Windows Server 2012 R2 Standart x64; - Microsoft Windows 10 Pro, 64-разрядная
3.	Прикладное программное обеспечение	- 1С: Предприятие Конфигурация: Зарплата и кадры бюджетного учреждения
4.	Средства защиты информации	**Средства антивирусной защиты:**

№ п/п	Характеристика	Значение характеристики
		- Kaspersky Endpoint Security для Windows (версия 11.1.1.126) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2024) **Средства криптографической защиты информации:** - Программный комплекс ViPNet Client 4 (версия 4.5) (исполнение 2) (Сертифицирующий орган ФСБ России № СФ/124-4062 от 18.05.2021 действителен до 18.05.2024)

3.2.2. ИСПДн «Бухгалтерский и кадровый учет» представляет собой локальную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в пределах одного здания (нескольких близко расположенных зданий) и объединенных в единую систему) со следующими характеристиками:

3.2.2.1. Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – отсутствует.

3.2.2.2. Подключение к информационно-телекоммуникационным сетям АУ «Нефтеюганский политехнический колледж» – отсутствует.

3.2.2.3. Подключение к информационно-телекоммуникационной сети «Интернет» – отсутствует.

3.2.2.4. Подключение к информационно-телекоммуникационным сетям иных организаций – отсутствует.

3.2.2.5. В ИСПДне «Бухгалтерский и кадровый учет» не осуществляется взаимодействие с системами и сетями других организаций.

3.2.2.6. В ИСПДне «Бухгалтерский и кадровый учет» не осуществляется взаимодействие с другими системами и сетями АУ «Нефтеюганский политехнический колледж».

3.2.2.7. К информационным ресурсам ИСПДна «Бухгалтерский и кадровый учет» не осуществляется локальный доступ.

3.2.2.8. К информационным ресурсам ИСПДна «Бухгалтерский и кадровый учет» не осуществляется удаленный доступ.

3.2.3. Технологии, используемые в ИСПДне «Бухгалтерский и кадровый учет» отражены в таблице 4.

Таблица 4 – Технологии, используемые в ИСПДне «Бухгалтерский и кадровый учет»

№ п/п	Технология	Используется / Не используется
1.	Съемные носители информации	Не используются
2.	Технология виртуализации	Используются
3.	Технология беспроводного доступа	Не используются
4.	Мобильные технические средства	Не используются
5.	Веб-серверы	Не используются
6.	Технология веб-доступа	Не используются

№ п/п	Технология	Используется / Не используется
7.	Smart-карты	Не используются
8.	Технологии грид-систем	Не используются
9.	Технологии суперкомпьютерных систем	Не используются
10.	Большие данные	Не используются
11.	Числовое программное оборудование	Не используются
12.	Одноразовые пароли	Не используются
13.	Технология передачи видеоинформации	Не используется
14.	Технология удаленного рабочего стола	Не используются
15.	Технология удаленного администрирования	Не используются
16.	Технология удаленного внеполосного доступа	Не используются
17.	Технология передачи речи	Не используются
18.	Технология искусственного интеллекта	Не используются

3.2.4. ИСПДн «Бухгалтерский и кадровый учет» функционирует на базе инфраструктуры АУ «Нефтеюганский политехнический колледж».

4. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

4.2. Негативные последствия определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивает ИСПДн «Бухгалтерский и кадровый учет», и применительно к нарушению безопасности информации, содержащейся в ИСПДне «Бухгалтерский и кадровый учет».

4.3. На основе анализа исходных данных ИСПДна «Бухгалтерский и кадровый учет» определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 5.

Таблица 5 – Виды рисков (ущерба) и негативные последствия

Идентификатор	Негативные последствия	Вид риска (ущерба)
НП.1	Разглашение персональных данных граждан	У1. Ущерб физическому лицу
НП.2	Нарушение неприкосновенности частной жизни	У1. Ущерб физическому лицу
НП.3	Нарушение личной, семейной тайны, утрата чести и доброго имени	У1. Ущерб физическому лицу
НП.4	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	У1. Ущерб физическому лицу
НП.5	Финансовый, иной материальный ущерб физическому лицу	У1. Ущерб физическому лицу
НП.6	Нарушение конфиденциальности (утечка) персональных данных	У1. Ущерб физическому лицу
НП.7	Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.8	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.9	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.10	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

Идентификатор	Негативные последствия	Вид риска (ущерба)
НП.11	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.12	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

5. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

5.1. В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты ИСПДна «Бухгалтерский и кадровый учет», несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, определенным в разделе 4 настоящей Модели угроз, – объектов воздействия.

5.2. Объекты воздействия определялись для реальной архитектуры и условий функционирования ИСПДна «Бухгалтерский и кадровый учет» на основе анализа исходных данных и проведенной инвентаризации.

5.3. Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

5.4. В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 6.

Таблица 6 – Виды воздействия

Идентификатор	Вид воздействия
ВВ.1	утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач
ВВ.6	нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

5.5. Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 7.

Таблица 7 – Объекты воздействия и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан	Узел вычислительной сети (автоматизированные	ВВ.2; ВВ.3; ВВ.4; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
Нарушение неприкосновенности частной жизни	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение личной, семейной тайны, утрата чести и доброго имени	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Финансовый, иной материальный ущерб физическому лицу	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
Нарушение конфиденциальности (утечка) персональных данных	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе	ВВ.1; ВВ.2; ВВ.3; ВВ.4

Негативные последствия	Объекты воздействия	Виды воздействия
	средств вычислительной техники	
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	BIOS/UEFI	ВВ.2; ВВ.3; ВВ.4
	Сетевое оборудование	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Микропрограммное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Система поддержания температурно-влажностного режима	ВВ.2; ВВ.3; ВВ.4
Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	BIOS/UEFI	ВВ.2; ВВ.3; ВВ.4
	Сетевое оборудование	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевое программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
	машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Микропрограммное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Система поддержания температурно-влажностного режима	ВВ.2; ВВ.3; ВВ.4
Необходимость изменения (перестроения) внутренних процедур	BIOS/UEFI	ВВ.2; ВВ.3; ВВ.4
	Сетевое оборудование	ВВ.2; ВВ.3; ВВ.4; ВВ.6

Негативные последствия	Объекты воздействия	Виды воздействия
для достижения целей, решения задач (реализации функций)	Сетевое программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Микропрограммное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4

Негативные последствия	Объекты воздействия	Виды воздействия
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Система поддержания температурно-влажностного режима	ВВ.2; ВВ.3; ВВ.4
Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4

6. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. Антропогенные источники

6.1.1. В ходе оценки угроз безопасности информации определяются возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие(ая) реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты ИСПДна «Бухгалтерский и кадровый учет», – актуальные нарушители.

6.1.2. Процесс определения актуальных нарушителей включал:

6.1.2.1. Формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предположений об их отнесении к числу возможных нарушителей (нарушителей, подлежащих дальнейшей оценке), представленных в таблице 8.

Таблица 8 – Перечень рассматриваемых нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
1.	Специальные службы иностранных государств	Нанесение ущерба государству в области обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций; Получение конкурентных преимуществ на уровне государства; Срыв заключения международных договоров; Создание внутриполитического кризиса	Цели не предполагают потенциальное наличие нарушителя
2.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций	Цели не предполагают потенциальное наличие нарушителя
3.	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды; Желание самореализации (подтверждение статуса)	Цели не предполагают потенциальное наличие нарушителя
4.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса)	Возможные цели реализации угроз безопасности информации

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
			предполагают наличие нарушителя
5.	Конкурирующие организации	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ	Цели не предполагают потенциальное наличие нарушителя
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия	Цели не предполагают потенциальное наличие нарушителя
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
8.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
10.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
11.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса);	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
		Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	
12.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
13.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

6.1.2.2. Определение характеристик (категория нарушителя и уровень возможности по реализации угроз безопасности информации) возможных нарушителей.

6.1.2.3. Оценка возможности привлечения (вхождения в сговор) одними нарушителями других (в том числе обладающих привилегированными правами доступа).

6.1.2.4. Сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации. По результатам сопоставления определяются актуальные нарушители по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ИСПДна «Бухгалтерский и кадровый учет» негативным последствиям и соответствующим рискам (видам ущерба).

6.1.3. Итоговые характеристики возможных нарушителей представлены в таблице 9.

Таблица 9 – Характеристики возможных нарушителей

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1.	Отдельные физические лица (хакеры)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
3.	Поставщики вычислительных услуг, услуг связи	Внутренний	Н2. Нарушитель, обладающий	Да

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
			базовыми повышенными возможностями	
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
6.	Авторизованные пользователи систем и сетей	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
7.	Системные администраторы и администраторы безопасности	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
8.	Бывшие (уволенные) работники (пользователи)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да

6.1.4. Категория нарушителя определяется исходя из следующих принципов:

– внешний нарушитель – если нарушитель не имеет прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам ИСПДна «Бухгалтерский и кадровый учет», требующим авторизации;

– внутренний нарушитель – если нарушитель имеет права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам ИСПДна «Бухгалтерский и кадровый учет». К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ИСПДна «Бухгалтерский и кадровый учет».

6.1.5. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

6.1.6. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных

характеристик определяет уровень возможностей нарушителя по реализации угроз безопасности информации.

6.1.7. Уровень возможности нарушителя определяется исходя из следующих принципов:

– нарушитель, обладающий базовыми возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов;

– нарушитель, обладающий базовыми повышенными возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий средними возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе на выявленные им неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий высокими возможностями по реализации угроз безопасности информации – если имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.

7. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

7.1. В ходе оценки угроз безопасности информации определяются возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ИСПДне «Бухгалтерский и кадровый учет», – актуальные способы реализации (возникновения) угроз безопасности информации.

7.2. Процесс определения актуальных способов реализации (возникновения) угроз безопасности информации включал:

7.2.1. Составление перечня рассматриваемых (возможных) способов реализации угроз безопасности. Перечень возможных способов реализации угроз безопасности информации представлен в таблице 10.

Таблица 10 – Перечень возможных способов реализации угроз безопасности информации

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного программного обеспечения
СР.3	Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
СР.4	Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
СР.6	Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.8	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.9	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств
СР.10	Перехват трафика сети передачи данных
СР.11	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
СР.12	Реализация атак типа "отказ в обслуживании" в отношении технических средств, программного обеспечения и каналов передачи данных

7.2.2. Определение интерфейсов объектов воздействия, определенных в соответствии с разделом 5 настоящей Модели угроз. Интерфейсы объектов воздействия определялись на основе изучения и анализа данных:

– об архитектуре, составе и условиях функционирования ИСПДна «Бухгалтерский и кадровый учет»;

– о группах пользователей ИСПДна «Бухгалтерский и кадровый учет», их типов доступа и уровней полномочий.

7.2.3. Определение наличия у актуальных нарушителей возможности доступа к интерфейсам объектов воздействия.

7.2.4. Определение актуальных способов реализации (возникновения) угроз безопасности информации актуальным нарушителем через доступные ему интерфейсы объектов воздействия.

7.3. Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации, включающие описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям, представлены в таблице 11.

Таблица 11 – Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
Отдельные физические лица (хакеры)	Внешний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Информационная (автоматизированная) система	Пользователи	СР.1
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
		Защищаемая информация	Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
Поставщики вычислительных услуг, услуг связи	Внутренний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Системное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Защищаемая информация	Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Информационная (автоматизированная) система	Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4
		Учетные данные пользователя	Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
		Прикладное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9
	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
		Защищаемая информация	Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.11
		Объекты файловой системы	Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9
Авторизованные пользователи систем и сетей	Внутренний	BIOS/UEFI	Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		База данных	Прикладное приложение, использующее базу данных	СР.1
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к виртуальным машинам	СР.1; СР.2
			Виртуальные каналы передачи данных	СР.10
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
Системные администраторы и администраторы безопасности	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к виртуальным машинам	СР.1; СР.2
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные ра-	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		бочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Информационная (автоматизированная) система	Процесс создания (модернизации) информационной (автоматизированной) системы	СР.4; СР.8; СР.9
			Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Канал удаленного администрирования СКЗИ	СР.1
Бывшие (уволенные) работники (пользователи)	Внешний	Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		данных, систему управления виртуальной инфраструктурой)		
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9

8. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

8.1. В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для ИСПДна «Бухгалтерский и кадровый учет» – актуальные угрозы безопасности информации.

8.2. Процесс определения актуальных угроз безопасности информации включал:

8.2.1. Выделение из исходного перечня угроз безопасности информации возможных угроз по следующему принципу: угроза безопасности информации признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

Перечень исключенных из исходного перечня угроз безопасности информации представлен в Приложении № 4.

8.2.2. Оценку возможных угроз на предмет актуальности по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

Сценарии определяются для соответствующих способов реализации угроз безопасности информации.

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации представлен в Приложении № 5.

8.3. По результатам оценки возможных угроз безопасности выявлено актуальных угроз: 131. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 12.

Таблица 12 – Актуальные угрозы безопасности информации

Идентификатор угрозы	**Наименование угрозы**
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями

Идентификатор угрозы	Наименование угрозы
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.033	Угроза использования слабостей кодирования входных данных
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.041	Угроза межсайтового скриптинга
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением

Идентификатор угрозы	Наименование угрозы
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.088	Угроза несанкционированного копирования защищаемой информации
УБИ.089	Угроза несанкционированного редактирования реестра
УБИ.090	Угроза несанкционированного создания учётной записи пользователя
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.103	Угроза определения типов объектов защиты
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.108	Угроза ошибки обновления гипервизора
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.111	Угроза передачи данных по скрытым каналам

Идентификатор угрозы	Наименование угрозы
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.128	Угроза подмены доверенного пользователя
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.156	Угроза утраты носителей информации
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.158	Угроза форматирования носителей информации
УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.162	Угроза эксплуатации цифровой подписи программного кода
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.169	Угроза наличия механизмов разработчика
УБИ.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети

Идентификатор угрозы	Наименование угрозы
УБИ.172	Угроза распространения «почтовых червей»
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
УБИ.179	Угроза несанкционированной модификации защищаемой информации
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
УБИ.182	Угроза физического устаревания аппаратных компонентов
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза перехвата управления информационной системой
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

9. ОЦЕНКА УГРОЗ В СООТВЕТСТВИИ С МЕТОДИЧЕСКИМИ ДОКУМЕНТАМИ ФСБ РОССИИ

9.1. На основании исходных данных об объектах защиты (в соответствии с разделом 5 настоящей Модели угроз) и источниках атак (в соответствии с разделом 6.1 настоящей Модели угроз) ИСПДна «Бухгалтерский и кадровый учет» определены обобщенные возможности источников атак (таблица 13).

Таблица 13 – Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Предположение о возможности источников атак
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

9.2. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности информации определяется возможностями источников атак.

9.3. Исходя из обобщенных возможностей источников атак определены уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы). Результаты приведены в Приложении № 7.

9.4. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КС3.

Источники разработки модели угроз

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

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– 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 Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;

– 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;

– 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 29099-91 «Сети вычислительные локальные. Термины и определения», утвержденный постановлением Комитета стандартизации и метрологии СССР от 25 сентября 1991 г. № 1491;

– ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1520-ст;

– ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1521-ст;

– ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. № 3469;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», утвержденный постановлением Госстандарта России от 9 февраля 1995 г. № 49;

– 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 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», утвержденный постановлением Госстандарта России от 14 июля 1998 г. № 295;

– 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 2.105-2019 «Единая система конструкторской документации. Общие требования к текстовым документам», утвержденный приказом Росстандарта от 29 апреля 2019 г. № 175-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 Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов», утвержденный приказом Росстандарта от 25 октября 2021 г. № 1297-ст;

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

Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности
1.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.6	НП.9; НП.10; НП.11; НП.12	–
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Получение конкурентных преимуществ	НП.6	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.6	НП.7; НП.8; НП.9	–
3.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Получение конкурентных преимуществ	–	НП.12	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.6	НП.7; НП.8; НП.9; НП.10; НП.12	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Получение конкурентных преимуществ	–	НП.12	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.6	НП.7; НП.8; НП.9; НП.10; НП.12	–
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.6	НП.7; НП.8; НП.9; НП.12	–
6.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.3; НП.6	НП.12	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.6	НП.7; НП.8; НП.9; НП.12	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.6	–	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
7.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.6	НП.12	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.6	НП.7; НП.8; НП.9; НП.10; НП.12	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.6	–	–
8.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды	НП.5; НП.6	–	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.6	–	–

Уровни возможностей нарушителя

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
Н1	Нарушитель, обладающий базовыми возможностями	– Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. – Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. – Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним
Н2	Нарушитель, обладающий базовыми повышенными возможностями	– Обладает всеми возможностями нарушителей с базовыми возможностями. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. – Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. – Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. – Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах
Н3	Нарушитель, обладающий средними возможностями	– Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. – Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. – Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа.

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
		– Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. – Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. – Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц
Н4	Нарушитель, обладающий высокими возможностями	– Обладает всеми возможностями нарушителей со средними возможностями. – Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». – Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. – Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. – Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. – Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. – Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. – Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей

Перечень исключенных из базового перечня угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Отсутствуют объекты воздействия
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Отсутствуют объекты воздействия
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Отсутствуют объекты воздействия
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Отсутствуют объекты воздействия
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Отсутствуют объекты воздействия
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Отсутствуют объекты воздействия
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.026	Угроза искажения XML-схемы	Отсутствуют объекты воздействия
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Отсутствуют объекты воздействия
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.040	Угроза конфликта юрисдикций различных стран	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.042	Угроза межсайтовой подделки запроса	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.043	Угроза нарушения доступности облачного сервера	Отсутствуют объекты воздействия
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Отсутствуют объекты воздействия
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Отсутствуют объекты воздействия
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Отсутствуют объекты воздействия
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Отсутствуют объекты воздействия
УБИ.055	Угроза незащищённого администрирования облачных услуг	Отсутствуют объекты воздействия
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Отсутствуют объекты воздействия
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Отсутствуют объекты воздействия
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Отсутствуют объекты воздействия
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Отсутствуют объекты воздействия
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Отсутствуют объекты воздействия
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Отсутствуют объекты воздействия
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Отсутствуют объекты воздействия
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Отсутствуют объекты воздействия
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Отсутствуют объекты воздействия
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.097	Угроза несогласованности правил доступа к большим данным	Отсутствуют объекты воздействия
УБИ.101	Угроза общедоступности облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Отсутствуют объекты воздействия
УБИ.107	Угроза отключения контрольных датчиков	Отсутствуют объекты воздействия
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Отсутствуют объекты воздействия
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Отсутствуют объекты воздействия
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Отсутствуют объекты воздействия
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Отсутствуют объекты воздействия
УБИ.127	Угроза подмены действия пользователя путём обмана	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.131	Угроза подмены субъекта сетевого доступа	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.132	Угроза получения предварительной информации об объекте защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Отсутствуют объекты воздействия
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Отсутствуют объекты воздействия
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Отсутствуют условия, при которых может быть реализована угроза

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.137	Угроза потери управления облачными ресурсами	Отсутствуют объекты воздействия
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Отсутствуют объекты воздействия
УБИ.139	Угроза преодоления физической защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.141	Угроза привязки к поставщику облачных услуг	Отсутствуют объекты воздействия
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Отсутствуют объекты воздействия
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Отсутствуют объекты воздействия
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Отсутствуют объекты воздействия
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Отсутствуют объекты воздействия
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Отсутствуют объекты воздействия
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Отсутствуют объекты воздействия
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Отсутствуют объекты воздействия
УБИ.173	Угроза «спама» веб-сервера	Отсутствуют объекты воздействия
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Отсутствуют объекты воздействия
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Отсутствуют объекты воздействия
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.189	Угроза маскирования действий вредоносного кода	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Отсутствуют объекты воздействия
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Отсутствуют объекты воздействия
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Отсутствуют объекты воздействия
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Отсутствуют объекты воздействия
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Отсутствуют объекты воздействия
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Отсутствуют объекты воздействия
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.213	Угроза обхода многофакторной аутентификации	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Отсутствуют объекты воздействия
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Отсутствуют объекты воздействия
УБИ.219	Угроза хищения обучающих данных	Отсутствуют объекты воздействия
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Отсутствуют объекты воздействия
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Отсутствуют объекты воздействия
УБИ.222	Угроза подмены модели машинного обучения	Отсутствуют объекты воздействия

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях	Т1.1 Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2 Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.3 Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4 Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.5 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств
		Т1.6 Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора
		Т1.7 Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		Т1.8 Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.9 Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.
		Т1.10 Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)
		Т1.11 Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга

№	Тактика	Основные техники
		T1.12 Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		T1.13 Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		T1.14 Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		T1.15 Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
		T1.16 Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров
		T1.17 Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.18 Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.19 Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.20 Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.21 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем анализа и обобщения информации перехватываемой в сети передачи информации
		T1.22 Поиск и покупка специализированного программного обеспечения (вредоносного кода) на специализированных нелегальных площадках

№	Тактика	Основные техники
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1 Использование внешних сервисов организации в сетях публичного доступа (Интернет)
		Т2.2 Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра
		Т2.3 Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.4 Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.5 Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке
		Т2.6 Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
		Т2.7 Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций
		Т2.8 Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.9 Несанкционированное подключение внешних устройств
		Т2.10 Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
		Т2.11 Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
		Т2.12 Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа
		Т2.13 Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки
		Т2.14 Доступ путем эксплуатации недостатков систем биометрической аутентификации
		Т2.15 Доступ путем использования недостатков правовых норм других стран, участвующих в трансграничной передаче облачного трафика

№	Тактика	Основные техники
		Т2.16 Доступ путем использования возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1 Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.2 Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
		Т3.3 Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
		Т3.4 Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
		Т3.5 Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
		Т3.6 Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
		Т3.7 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т3.8 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т3.9 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т3.10 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т3.11 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «даркверб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т3.12 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы

№	Тактика	Основные техники
		Т3.13 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.14 Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		Т3.15 Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
		Т3.16 Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL
		Т3.17 Планирование запуска вредоносного кода при запуске компьютера путем эксплуатации стандартных механизмов BIOS (UEFI) и т.п.
		Т3.18 Эксплуатация уязвимостей типа локальное исполнение программного кода
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1 Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2 Использование штатных средств удаленного доступа и управления операционной системы
		Т4.3 Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода
		Т4.4 Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
		Т4.5 Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети
		Т4.6 Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
		Т4.7 Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей

№	Тактика	Основные техники
		T4.8 Использование прошивок устройств с уязвимостями, к примеру, внедрение новых функций в BIOS (UEFI)
T5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	T5.1 Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		T5.2 Использование штатных средств удаленного доступа и управления операционной системы
		T5.3 Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		T5.4 Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		T5.5 Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		T5.6 Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения
		T5.7 Туннелирование трафика управления через VPN
		T5.8 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		T5.9 Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
		T5.10 Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
		T5.11 Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		T5.12 Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.
		T5.13 Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения
T6	Повышение привилегий по доступу к	T6.1 Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими

№	Тактика	Основные техники
	компонентам систем и сетей	Т6.2 Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий
		Т6.4 Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи)
		Т6.5 Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций
		Т6.6 Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима
		Т6.7 Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями
		Т6.8 Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей
		Т6.9 Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1 Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения
		Т7.2 Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3 Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4 Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
		Т7.5 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
		Т7.6 Подделка данных вывода средств защиты от угроз информационной безопасности
		Т7.7 Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности,

№	Тактика	Основные техники
		иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
		Т7.8 Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки
		Т7.9 Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей
		Т7.10 Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
		Т7.11 Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе
		Т7.12 Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности
		Т7.13 Создание скрытых файлов, скрытых учетных записей
		Т7.14 Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
		Т7.15 Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
		Т7.16 Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки
		Т7.17 Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети
		Т7.18 Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе
		Т7.19 Туннелирование трафика управления через VPN
		Т7.20 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие

№	Тактика	Основные техники
		Т7.21 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22 Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т7.24 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т7.25 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т7.26 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т7.27 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т7.29 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или	Т8.1 Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
		Т8.2 Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
		Т8.3 Использование механизмов дистанционной установки программного обеспечения и конфигурирования
		Т8.4 Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям

№	Тактика	Основные техники
	смежным системам и сетям	T8.5 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		T8.6 Копирование вредоносного кода на съемные носители
		T8.7 Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
		T8.8 Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях
T9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	T9.1 Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		T9.2 Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		T9.3 Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		T9.4 Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		T9.5 Отправка данных по известным протоколам управления и передачи данных
		T9.6 Отправка данных по собственным протоколам
		T9.7 Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения
		T9.8 Туннелирование трафика передачи данных через VPN
		T9.9 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		T9.10 Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		T9.11 Отправка данных через альтернативную среду передачи данных
		T9.12 Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации

№	Тактика	Основные техники
		Т9.13 Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
		Т9.14 Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1 Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		Т10.2 Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		Т10.3 Несанкционированное воздействие на программные модули прикладного программного обеспечения
		Т10.4 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
		Т10.5 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения
		Т10.6 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства
		Т10.7 Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
		Т10.8 Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
		Т10.9 Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.10 Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
		Т10.11 Нецелевое использование ресурсов системы
		Т10.12 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.13 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов,

№	Тактика	Основные техники
		представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		T10.14 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		T10.15 Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой

Результаты оценки возможных угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средства криптографической защиты информации	НП.6; НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.003: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т10 (Т10.2; Т10.5)
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.9; СР.11	Сценарий реализации УБИ.004: – Т1 (Т1.9; Т1.15; Т1.16); – Т2 (Т2.9)
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.006: – Т1 (Т1.4; Т1.5); – Т2 (Т2.5; Т2.10); – Т3 (Т3.1; Т3.2; Т3.15); – Т4 (Т4.2); – Т5 (Т5.2)
УБИ.007	Угроза воздействия на прог-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11;	СР.1; СР.3; СР.9	Сценарий реализации УБИ.007: – Т1 (Т1.9; Т1.16); – Т2 (Т2.6);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	раммы с высокими привилегиями		обеспечение, Прикладное программное обеспечение	НП.12		– Т3 (Т3.5); – Т6 (Т6.2; Т6.3)
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Микропрограммное обеспечение, Учетные данные пользователя	НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.008: – Т1 (Т1.6); – Т2 (Т2.10); – Т4 (Т4.1)
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.8; СР.9	Сценарий реализации УБИ.009: – Т1 (Т1.9); – Т3 (Т3.18); – Т4 (Т4.8)
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.2	Сценарий реализации УБИ.010: – Т1 (Т1.5; Т1.9; Т1.16; Т1.22); – Т2 (Т2.5; Т2.6); – Т3 (Т3.1; Т3.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Объекты файловой системы, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.3; СР.9	Сценарий реализации УБИ.012: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5; Т2.6); – Т3 (Т3.7)
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.013: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.), Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.3; СР.9	Сценарий реализации УБИ.014: – Т1 (Т1.5; Т1.16; Т1.19); – Т2 (Т2.5; Т2.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.6; НП.10; НП.11; НП.12	СР.1; СР.3	Сценарий реализации УБИ.015: – Т1 (Т1.9; Т1.16); – Т2 (Т2.3; Т2.5; Т2.6); – Т6 (Т6.3; Т6.6)
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.018: – Т2 (Т2.5); – Т10 (Т10.2)
УБИ.019	Угроза заражения DNS-кеша	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.019: – Т8 (Т8.8)
УБИ.022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение	НП.9; НП.10; НП.11	СР.2; СР.4	Сценарий реализации УБИ.022: – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.2; Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Средство вычислительной техники, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.4	Сценарий реализации УБИ.023: – Т2 (Т2.7); – Т3 (Т3.7); – Т10 (Т10.3)
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.3	Сценарий реализации УБИ.025: – Т10 (Т10.2; Т10.4)
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2; СР.3	Сценарий реализации УБИ.027: – Т3 (Т3.2); – Т8 (Т8.1)
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.6; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.028: – Т1 (Т1.5; Т1.9); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.030: – Т1 (Т1.1; Т1.9; Т1.16); – Т2 (Т2.4)
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.8	Сценарий реализации УБИ.031: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.4; Т2.5); – Т6 (Т6.3; Т6.6)
УБИ.033	Угроза использования слабостей кодирования входных данных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.033: – Т1 (Т1.5); – Т2 (Т2.5; Т2.6); – Т10 (Т10.2)
УБИ.034	Угроза использования слабостей про-	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Сетевое программное обеспечение, Сетевой трафик, Системное	НП.4; НП.5; НП.6; НП.9; НП.10; НП.11;	СР.1; СР.3	Сценарий реализации УБИ.034: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	токолов сетевого/локального обмена данными	Внутренний нарушитель, обладающий базовыми повышенными возможностями	программное обеспечение	НП.12		– Т10 (Т10.1)
УБИ.036	Угроза исследования механизмов работы программы	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.8	Сценарий реализации УБИ.036: – Т2 (Т2.5)
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.037: – Т1 (Т1.9); – Т2 (Т2.5; Т2.6)
УБИ.041	Угроза межсайтового скриптинга	Внешний нарушитель, обладающий базовыми возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.041: – Т1 (Т1.1; Т1.5; Т1.8); – Т2 (Т2.1); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.2	Сценарий реализации УБИ.044: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.3; Т2.5); – Т3 (Т3.1); – Т10 (Т10.2; Т10.3)
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1	Сценарий реализации УБИ.045: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6); – Т10 (Т10.2; Т10.6)
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.046: – Т2 (Т2.4; Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.048: – Т2 (Т2.3; Т2.5); – Т3 (Т3.7); – Т4 (Т4.3; Т4.5; Т4.7); – Т10 (Т10.2; Т10.7)
УБИ.049	Угроза нарушения целостности данных кеша	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.049: – Т2 (Т2.5); – Т3 (Т3.9); – Т10 (Т10.1; Т10.2)
УБИ.051	Угроза невозможности восстановления	Внутренний нарушитель, обладающий базовыми возможностями,	Узел вычислительной сети (автоматизиро-	НП.1; НП.6; НП.9; НП.10;	СР.9	Сценарий реализации УБИ.051: – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель, обладающий базовыми повышенными возможностями	ванные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.11; НП.12		
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.11	Сценарий реализации УБИ.053: – Т2 (Т2.5)
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8; СР.9	Сценарий реализации УБИ.059: – Т10 (Т10.10)
УБИ.061	Угроза некорректного за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, База данных	НП.2; НП.3; НП.4; НП.5; НП.6; НП.8; НП.9;	СР.1; СР.9	Сценарий реализации УБИ.061: – Т1 (Т1.5); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	дания структуры данных транзакции			НП.10; НП.11; НП.12		
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.2; СР.9	Сценарий реализации УБИ.062: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.063: – Т2 (Т2.5); – Т10 (Т10.11)
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.6; НП.8; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.067: – Т1 (Т1.13; Т1.14); – Т10 (Т10.1)
УБИ.068	Угроза неправомерного/некорректного использования интерфейса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Мик-	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.068: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	взаимодействия с приложением		ропрограммное обеспечение, Прикладное программное обеспечение			
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.6; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.069: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.071: – Т1 (Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.072: – Т2 (Т2.5); – Т3 (Т3.8; Т3.18); – Т4 (Т4.6)
УБИ.073	Угроза несанкционированного доступа к активному и	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Сетевое программное обеспечение, Виртуальная ин-	НП.9; НП.10; НП.11	СР.1; СР.2; СР.9	Сценарий реализации УБИ.073: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	(или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети		фраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой), Микропрограммное обеспечение			
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Машинный носитель информации в составе средств вычислительной техники, Учетные данные пользователя, Объекты файловой системы	НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.074: – Т1 (Т1.12); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.075	Угроза несанкционированного доступа к виртуальным	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.075: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	каналам передачи	Внутренний нарушитель, обладающий базовыми повышенными возможностями	шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.076: – Т10 (Т10.10)
УБИ.077	Угроза несанкционированного доступа к данным за пределами за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы вирту-	НП.9; НП.10; НП.11	СР.1; СР.2	Сценарий реализации УБИ.077: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.1); – Т4 (Т4.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	резервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение		альных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			– Т7 (Т7.18); – Т10 (Т10.1; Т10.11)
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8; СР.9	Сценарий реализации УБИ.078: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства,	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.079: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	стороны других виртуальных машин		виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.080: – Т1 (Т1.5; Т1.16); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.084: – Т1 (Т1.5; Т1.22)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.6; НП.8; НП.12	СР.1; СР.8	Сценарий реализации УБИ.085: – Т1 (Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Учетные данные пользователя, Объекты файловой системы	НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.086: – Т1 (Т1.5; Т1.12; Т1.22); – Т2 (Т2.4; Т2.11); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.087: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.6; НП.8; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.088: – Т2 (Т2.4; Т2.9); – Т10 (Т10.1)
УБИ.089	Угроза несанкционированного редактирования реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.089: – Т1 (Т1.5; Т1.9); – Т2 (Т2.4); – Т4 (Т4.5); – Т10 (Т10.1)
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.090: – Т1 (Т1.5); – Т2 (Т2.4); – Т4 (Т4.1); – Т5 (Т5.2); – Т10 (Т10.2)
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.6; НП.8; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.091: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.093: – Т1 (Т1.9); – Т2 (Т2.4; Т2.5); – Т3 (Т3.2); – Т10 (Т10.1)
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.094: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1; Т10.3)
УБИ.095	Угроза несанкционированного управления указателями	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.095: – Т1 (Т1.5); – Т2 (Т2.4; Т2.11); – Т3 (Т3.2); – Т10 (Т10.3; Т10.4)
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы,	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.098: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			коммутаторы, IoT-устройства и т.п.)			
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.099: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.8; СР.9	Сценарий реализации УБИ.100: – Т2 (Т2.4; Т2.5); – Т4 (Т4.1); – Т6 (Т6.6)
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.102: – Т2 (Т2.5)
УБИ.103	Угроза определения типов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой	НП.1; НП.4; НП.5; НП.6; НП.9;	СР.8; СР.9	Сценарий реализации УБИ.103: – Т1 (Т1.1; Т1.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	объектов защиты		трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.10; НП.11; НП.12		– Т2 (Т2.4)
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.104: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3)
УБИ.108	Угроза ошибки обновления гипервизора	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.108: – Т2 (Т2.5); – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			инфраструктурой)			
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.109: – Т2 (Т2.5; Т2.6); – Т10 (Т10.10)
УБИ.111	Угроза передачи данных по скрытым каналам	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик, Системное программное обеспечение	НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.111: – Т2 (Т2.4); – Т9 (Т9.10)
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.113: – Т2 (Т2.5; Т2.11); – Т10 (Т10.8)
УБИ.114	Угроза переполнения целочисленных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.114: – Т1 (Т1.1; Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.115: – Т1 (Т1.4; Т1.12); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т10 (Т10.1; Т10.3)
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.6; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.116: – Т1 (Т1.3); – Т2 (Т2.4; Т2.5; Т2.11)
УБИ.117	Угроза перехвата привилегированного потока	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.117: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т6 (Т6.1); – Т10 (Т10.1)
УБИ.118	Угроза перехвата привилегированного процесса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.118: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т6 (Т6.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.119	Угроза перехвата управления гипервизором	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.119: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)
УБИ.120	Угроза перехвата управления средой виртуализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.120: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.121	Угроза повреждения системного реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.6; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.121: – Т2 (Т2.4; Т2.5; Т2.11); – Т10 (Т10.8; Т10.10)
УБИ.122	Угроза повышения привилегий	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.2; СР.8	Сценарий реализации УБИ.122: – Т2 (Т2.5); – Т3 (Т3.5); – Т6 (Т6.1); – Т10 (Т10.3)
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.123: – Т1 (Т1.6); – Т2 (Т2.5; Т2.10); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации, Объекты файловой системы, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.124: – Т1 (Т1.22); – Т2 (Т2.5; Т2.11); – Т7 (Т7.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.128	Угроза подмены доверенного пользователя	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.128: – Т1 (Т1.5); – Т2 (Т2.5; Т2.9)
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.129: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.7); – Т4 (Т4.6; Т4.7)
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Прикладное программное обеспечение	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.130: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.2)
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера,	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9; СР.12	Сценарий реализации УБИ.140: – Т2 (Т2.3; Т2.5); – Т10 (Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Машинный носитель информации в составе средств вычислительной техники, Микропрограммное обеспечение	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.143: – Т1 (Т1.5); – Т2 (Т2.5); – Т7 (Т7.8); – Т10 (Т10.10)
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1	Сценарий реализации УБИ.144: – Т1 (Т1.9; Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.6)
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.145: – Т2 (Т2.4; Т2.5; Т2.8); – Т3 (Т3.3)
УБИ.149	Угроза сбоя обработки специ-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Объекты файловой системы	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.4	Сценарий реализации УБИ.149: – Т1 (Т1.5); – Т2 (Т2.5);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	альным образом изменённых файлов					– Т10 (Т10.10)
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.9	Сценарий реализации УБИ.150: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Микропрограммное обеспечение, Учетные данные пользователя	НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.152: – Т1 (Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.10)
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.153: – Т1 (Т1.2; Т1.22); – Т2 (Т2.3; Т2.5)
УБИ.154	Угроза установки уязвимых версий об-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.154: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.8);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	новления программного обеспечения BIOS					– Т4 (Т4.6); – Т7 (Т7.22); – Т10 (Т10.6; Т10.10)
УБИ.155	Угроза утраты вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.), Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.155: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5; Т2.11); – Т10 (Т10.10)
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8; СР.9	Сценарий реализации УБИ.156: – Т1 (Т1.10); – Т10 (Т10.1; Т10.8)
УБИ.157	Угроза физического выведения из строя средств	Внешний нарушитель, обладающий базовыми возможностями	Сетевое оборудование, Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9; СР.11	Сценарий реализации УБИ.157: – Т2 (Т2.2); – Т10 (Т10.8; Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	хранения, обработки и (или) ввода/вывода/передачи информации					
УБИ.158	Угроза форматирования носителей информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.158: – Т2 (Т2.2; Т2.5); – Т10 (Т10.8)
УБИ.159	Угроза «форсированного веб-браузинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.159: – Т2 (Т2.1; Т2.5); – Т10 (Т10.1)
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями	Сетевое оборудование, Средство вычислительной техники, Машинный носитель информации в составе средств вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.160: – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.4	Сценарий реализации УБИ.162: – Т1 (Т1.10); – Т3 (Т3.11; Т3.16)
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.163: – Т1 (Т1.3); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.7; НП.9; НП.10; НП.11	СР.9	Сценарий реализации УБИ.165: – Т2 (Т2.5)
УБИ.166	Угроза внедрения системной избыточности	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.7; НП.9; НП.10; НП.11	СР.9	Сценарий реализации УБИ.166: – Т2 (Т2.5)
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.2; СР.8	Сценарий реализации УБИ.167: – Т2 (Т2.4); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			т.п.)			
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Учетные данные пользователя	НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.168: – Т4 (Т4.1)
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.169: – Т2 (Т2.5; Т2.6); – Т3 (Т3.12)
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель, обладающий базовыми возможностями	Объекты файловой системы	НП.6; НП.10; НП.11; НП.12	СР.4	Сценарий реализации УБИ.170: – Т2 (Т2.4); – Т3 (Т3.3); – Т10 (Т10.8)
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, обладающий базовыми возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.6; НП.9; НП.10; НП.11; НП.12	СР.2; СР.8	Сценарий реализации УБИ.171: – Т1 (Т1.2); – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.1); – Т4 (Т4.3)
УБИ.172	Угроза распространения «почтовых червей»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.2; СР.8	Сценарий реализации УБИ.172: – Т1 (Т1.1); – Т2 (Т2.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.174	Угроза «фарминга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.174: – Т1 (Т1.1; Т1.8); – Т3 (Т3.3)
УБИ.175	Угроза «фишинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.175: – Т1 (Т1.1; Т1.11); – Т2 (Т2.8)
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Внешний нарушитель, обладающий базовыми возможностями	Средство защиты информации	НП.9; НП.10; НП.11	СР.1; СР.8; СР.12	Сценарий реализации УБИ.176: – Т10 (Т10.3; Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.177: – Т10 (Т10.14)
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.3	Сценарий реализации УБИ.178: – Т2 (Т2.4; Т2.5); – Т10 (Т10.5)
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.6; НП.10; НП.11; НП.12	СР.8; СР.11	Сценарий реализации УБИ.179: – Т2 (Т2.5); – Т10 (Т10.7; Т10.8)
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Система поддержания температурно-влажностного режима	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.180: – Т10 (Т10.14)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.182: – Т10 (Т10.8; Т10.10)
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.185: – Т2 (Т2.4); – Т7 (Т7.4)
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.2; СР.8	Сценарий реализации УБИ.186: – Т1 (Т1.1); – Т3 (Т3.3)
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации	НП.9; НП.10; НП.11	СР.1; СР.8; СР.9	Сценарий реализации УБИ.187: – Т2 (Т2.4); – Т7 (Т7.4); – Т10 (Т10.2)
УБИ.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11;	СР.2; СР.9	Сценарий реализации УБИ.188: – Т2 (Т2.7); – Т3 (Т3.7; Т3.8; Т3.10);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			обеспечение, Прикладное программное обеспечение	НП.12		– Т7 (Т7.24); – Т10 (Т10.7)
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.2; СР.8; СР.9	Сценарий реализации УБИ.191: – Т3 (Т3.2)
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.9	Сценарий реализации УБИ.192: – Т2 (Т2.5); – Т10 (Т10.2)
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2; СР.8	Сценарий реализации УБИ.203: – Т2 (Т2.5); – Т3 (Т3.2); – Т6 (Т6.3); – Т9 (Т9.11)
УБИ.205	Угроза нарушения работы компьютера и бло-	Внешний нарушитель, обладающий базовыми возможностями	Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.8	Сценарий реализации УБИ.205: – Т2 (Т2.4)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	кирования доступа к его данным из-за некорректной работы установленных на нем средств защиты					
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.2; СР.8	Сценарий реализации УБИ.208: – Т10 (Т10.11)
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.6; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.209: – Т10 (Т10.1; Т10.5)
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение	НП.9; НП.10; НП.11	СР.1; СР.9	Сценарий реализации УБИ.211: – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	конфигурационного файла, используемого программным обеспечением администрирования информационных систем					
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение, Средство вычислительной техники, Информационная (автоматизированная) система	НП.1; НП.6; НП.7; НП.9; НП.10; НП.11; НП.12	СР.1	Сценарий реализации УБИ.212: – Т2 (Т2.4; Т2.5); – Т8 (Т8.1); – Т10 (Т10.1)
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.7; НП.9; НП.10; НП.11	СР.1; СР.8	Сценарий реализации УБИ.214: – Т7 (Т7.4)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	события безопасности информации					
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение, Микропрограммное обеспечение, Прикладное программное обеспечение	НП.1; НП.5; НП.6; НП.9; НП.10; НП.11; НП.12	СР.1; СР.2	Сценарий реализации УБИ.217: – Т3 (Т3.8); – Т7 (Т7.24)

Уточненные возможности нарушителей и направления атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн «Бухгалтерский и кадровый учет», не имеют возможности находиться в помещениях, где расположена ИСПДн «Бухгалтерский и кадровый учет», в отсутствие пользователей ИСПДн «Бухгалтерский и кадровый учет»; – Работа пользователей ИСПДн «Бухгалтерский и кадровый учет» регламентирована; – Ответственный за обеспечение безопасности ПДн, администраторы ИСПДн «Бухгалтерский и кадровый учет» назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИСПДн «Бухгалтерский и кадровый учет», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Проводится обучение пользователей ИСПДн «Бухгалтерский и кадровый учет» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ	Да	– Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц; – Документация на СКЗИ не хранится у ответственного пользователя криптосредств в металлическом сейфе (шкафу); – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Нет	– Работа пользователей ИСПДн «Бухгалтерский и кадровый учет» регламентирована; – Проводится обучение пользователей ИСПДн «Бухгалтерский и кадровый учет» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Сведения о физических мерах защиты объектов, в которых размещена ИСПДн «Бухгалтерский и кадровый учет», доступны ограниченному кругу сотрудников

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Да	– Работа пользователей ИСПДн «Бухгалтерский и кадровый учет» регламентирована; – Ответственный за обеспечение безопасности ПДн, администраторы ИСПДн «Бухгалтерский и кадровый учет» назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИСПДн «Бухгалтерский и кадровый учет», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – Проводится обучение пользователей ИСПДн «Бухгалтерский и кадровый учет» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Пользователи ИСПДн «Бухгалтерский и кадровый учет» имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по обеспечению безопасности персональных данных
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИСПДн «Бухгалтерский и кадровый учет», не имеют возможности находиться в помещениях, где расположена ИСПДн «Бухгалтерский и кадровый учет», в отсутствие пользователей ИСПДн «Бухгалтерский и кадровый учет»; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
2.2	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 действий	Да	– В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода; – Корпуса системных блоков не защищены от вскрытия (не опечатаны/не опломбированы)
3.1	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
3.2	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
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	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
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			Высокая стоимость и сложность подготовки реализации возможности
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	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

Утверждена приказом АУ
«Нефтеюганский политехнический
колледж» от 18.11.2022 № 01-01-06/567

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Информационная система «Сайт»

г. Нефтеюганск
2022

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Архитектура – совокупность основных структурно-функциональных характеристик, свойств, компонентов ИС «Сайт», воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при ее обработке в информационных системах.

Взаимодействующая (смежная) система – система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с ИС «Сайт» и не включена оператором системы или сети в границу процесса оценки угроз безопасности информации.

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.

Возможности нарушителя – мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

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

Информация – данные, содержащиеся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.).

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть (ИТКС) – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные ресурсы – информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент – программное, программно-аппаратное или техническое средство, входящее в состав ИС «Сайт».

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

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.

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.

Обеспечивающие системы – инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Основные (критические) процессы (бизнес-процессы) – управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

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

Побочные электромагнитные излучения и наводки (ПЭМИН) – 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.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

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

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.

Программно-аппаратное средство – устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

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

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Средства криптографической защиты информации (шифровальные (криптографические) средства, криптосредства, СКЗИ) – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

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

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

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

Угроза безопасности информации (УБИ) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

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

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

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Введение

2.1.1. Настоящая модель угроз безопасности информации (далее – Модель угроз) содержит результаты оценки угроз безопасности информации.

2.1.2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в информационной системе «Сайт» (далее – ИС «Сайт») (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой в ИС «Сайт» информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования ИС «Сайт» – актуальных угроз безопасности информации.

2.1.3. В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» настоящая Модель угроз подлежит использованию при формировании требований к системе защиты ПДн, обрабатываемых в ИС «Сайт».

2.2. Источники разработки

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

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

– в случае определения АУ «Нефтеюганский политехнический колледж» (далее – АУ «Нефтеюганский политехнический колледж») необходимости обеспечения безопасности информации с использованием СКЗИ при формировании Модели угроз используются методические документы ФСТЭК России и ФСБ России.

2.3. Оцениваемые угрозы

2.3.1. Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (далее – ТКУИ), по причинам, перечисленным в таблице 1.

Таблица 1 – Обоснования исключения угроз, реализуемых за счет ТКУИ

№ п/п	Угрозы, связанные с техническими каналами утечки информации	Обоснование исключения
1.	Угрозы утечки акустической (речевой) информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящую специализированную аппаратуру, регистрирующую акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные (в том числе оптические) излучения и электрические сигналы, модулированные информативным акустическим сигналом, возникающие за счет преобразований в технических средствах обработки информации, ВТСС и строительных конструкциях и инженерно-технических коммуникациях под воздействием акустических волн. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
2.	Угрозы утечки видовой информации*	Характеризуются наличием высококвалифицированных нарушителей, использующих специализированные оптические (оптико-электронные) средства для просмотра информации с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз
3.	Угрозы утечки информации по каналам ПЭМИН	Характеризуются наличием высококвалифицированных нарушителей, использующих дорогостоящие специализированные технические средства перехвата побочных (не связанных с прямым функциональным значением элементов системы) информативных электромагнитных полей и электрических сигналов, возникающих при обработке информации техническими средствами системы. Характер и объем обрабатываемой в системе информации недостаточен для мотивации нарушителей к реализации таких угроз

* За исключением угроз, характеризующихся использованием нарушителями портативных (мобильных) устройств съема информации (планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

2.4. Ответственность за обеспечение защиты информации (безопасности)

2.4.1. Ответственными за обеспечение безопасности ПДн при их обработке в ИС «Сайт» приказом Директора АУ «Нефтеюганский политехнический колледж» назначены должностные лица / подразделения, представленные в таблице 2.

Таблица 2 – Ответственные за обеспечение защиты информации (безопасности)

№ п/п	Роль подразделения / должностного лица	Должностное лицо / подразделение
1.	Ответственный за обеспечение безопасности персональных данных	заведующий отделом информационных технологий

2.5. Особенности пересмотра Модели угроз

2.5.1. Настоящая Модель угроз может быть пересмотрена:

– по решению АУ «Нефтеюганский политехнический колледж» на основе периодически проводимых анализа и оценки угроз безопасности защищаемой информации с учетом особенностей и (или) изменений ИС «Сайт»;

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

– в случае изменения федерального законодательства в части оценки угроз безопасности информации;

– в случае появления новых угроз в используемых источниках данных об угрозах безопасности информации;

– в случае изменения структурно-функциональных характеристик, применяемых информационных технологий или особенностей функционирования ИС «Сайт»;

– в случае появления сведений и (или) фактов о новых возможностях потенциальных нарушителей;

– в случаях выявления инцидентов информационной безопасности в ИС «Сайт» и (или) взаимодействующих (смежных) системах.

3. ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

3.1. Общее описание объекта оценки угроз

3.1.1. Настоящая Модель угроз разработана в отношении ИС «Сайт».

3.1.2. Основные характеристики ИС «Сайт»:

3.1.3. Состав обрабатываемой информации:

– Персональные данные.

3.1.4. Основные процессы (бизнес-процессы), для обеспечения которых создана ИС «Сайт»:

– Осуществление расчета за оказание платных услуг (Предполагает обработку персональных данных с целью исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных).

3.1.5. Уровень защищенности ПДн: 4

3.2. Состав и архитектура объекта оценки

3.2.1. Состав ИС «Сайт» определен в таблице 3.

Таблица 3 – Состав ИС «Сайт»

№ п/п	Характеристика	Значение характеристики
1.	Программно-аппаратные средства	Отдел кадров ПК1 – 1 Отдел кадров ПК 2 – 1 Бухгалтерия ПК 1 – 1 Бухгалтерия ПК 2 – 1 Бухгалтерия ПК 3 – 1 Бухгалтерия ПК 4 – 1 Бухгалтерия ПК 5 – 1 Сервер DNS – 1 Контроллер домена – 2 файловый сервер – 1 Почтовый сервер – 1
2.	Общесистемное программное обеспечение	Операционные системы: - Debian GNU/Linux; - Microsoft Windows Server 2019 Standart, русская версия; - Microsoft Windows Server 2016 Standard; - Microsoft Windows 10 Pro, 64-разрядная
3.	Прикладное программное обеспечение	- Сайт
4.	Средства защиты информации	**Средства антивирусной защиты:** - Kaspersky Endpoint Security для Windows (версия 11.1.1.126) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2024) **Средства криптографической защиты информации:** - Программный комплекс ViPNet Client 4 (версия 4.5) (исполнение 2) (Сертифицирующий орган ФСБ России № СФ/124-4062 от 18.05.2021 действителен до 18.05.2024)

3.2.2. ИС «Сайт» представляет собой локальную систему (комплекс автоматизированных рабочих мест, коммуникационного и серверного оборудования, территориально размещенных в пределах одного здания (нескольких близко расположенных зданий) и объединенных в единую систему) со следующими характеристиками:

3.2.2.1. Подключение к сетям электросвязи, включенным в состав единой сети электросвязи Российской Федерации – присутствует, в соответствии с таблицей 4.

Таблица 4 – Подключения к сетям 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, беспроводной, протоколы TCP/IP, HTTP, POP3, FTP, SMTP, IMAP4
2.	общего пользования	ООО Интелком	оказание услуг	Тип доступа проводной, протоколы FTP, HTTP, IMAP4, POP3, SMTP, TCP/IP

3.2.2.2. Подключение к информационно-телекоммуникационным сетям АУ «Нефтеюганский политехнический колледж» – отсутствует.

3.2.2.3. Подключение к информационно-телекоммуникационной сети «Интернет» – отсутствует.

3.2.2.4. Подключение к информационно-телекоммуникационным сетям иных организаций – отсутствует.

3.2.2.5. В ИС «Сайт» не осуществляется взаимодействие с системами и сетями других организаций.

3.2.2.6. В ИС «Сайт» не осуществляется взаимодействие с другими системами и сетями АУ «Нефтеюганский политехнический колледж».

3.2.2.7. К информационным ресурсам ИС «Сайт» не осуществляется локальный доступ.

3.2.2.8. К информационным ресурсам ИС «Сайт» не осуществляется удаленный доступ.

3.2.3. Технологии, используемые в ИС «Сайт» отражены в таблице 5.

Таблица 5 – Технологии, используемые в ИС «Сайт»

№ п/п	Технология	Используется / Не используется
1.	Съемные носители информации	Не используются
2.	Технология виртуализации	Используются
3.	Технология беспроводного доступа	Не используются
4.	Мобильные технические средства	Не используются
5.	Веб-серверы	Используются

№ п/п	Технология	Используется / Не используется
6.	Технология веб-доступа	Не используются
7.	Smart-карты	Не используются
8.	Технологии грид-систем	Не используются
9.	Технологии суперкомпьютерных систем	Не используются
10.	Большие данные	Не используются
11.	Числовое программное оборудование	Не используются
12.	Одноразовые пароли	Не используются
13.	Электронная почта	Не используется
14.	Технология передачи видеоинформации	Используются
15.	Технология удаленного рабочего стола	Не используются
16.	Технология удаленного администрирования	Не используются
17.	Технология удаленного внеполосного доступа	Не используются
18.	Технология передачи речи	Не используются
19.	Технология искусственного интеллекта	Не используются

3.2.4. ИС «Сайт» функционирует на базе инфраструктуры АУ «Нефтеюганский политехнический колледж».

4. ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. В ходе оценки угроз безопасности информации определяются негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

4.2. Негативные последствия определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивает ИС «Сайт», и применительно к нарушению безопасности информации, содержащейся в ИС «Сайт».

4.3. На основе анализа исходных данных ИС «Сайт» определены негативные последствия, которые приводят к видам рисков (ущерба), представленные в таблице 6.

Таблица 6 – Виды рисков (ущерба) и негативные последствия

Идентификатор	**Негативные последствия**	**Вид риска (ущерба)**
НП.1	Разглашение персональных данных граждан	У1. Ущерб физическому лицу
НП.2	Нарушение неприкосновенности частной жизни	У1. Ущерб физическому лицу
НП.3	Нарушение личной, семейной тайны, утрата чести и доброго имени	У1. Ущерб физическому лицу
НП.4	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	У1. Ущерб физическому лицу
НП.5	Нарушение конфиденциальности (утечка) персональных данных	У1. Ущерб физическому лицу
НП.6	Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.7	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью
НП.8	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	У2. Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью

5. ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

5.1. В ходе оценки угроз безопасности информации определяются информационные ресурсы и компоненты ИС «Сайт», несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, определенным в разделе 4 настоящей Модели угроз, – объектов воздействия.

5.2. Объекты воздействия определялись для реальной архитектуры и условий функционирования ИС «Сайт» на основе анализа исходных данных и проведенной инвентаризации.

5.3. Определение объектов воздействия производилось на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей.

5.4. В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 7.

Таблица 7 – Виды воздействия

Идентификатор	Вид воздействия
ВВ.1	утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач
ВВ.6	нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

5.5. Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 8.

Таблица 8 – Объекты воздействия и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4

Негативные последствия	Объекты воздействия	Виды воздействия
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
Нарушение неприкосновенности частной жизни	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение личной, семейной тайны, утрата чести и доброго имени	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
Нарушение конфиденциальности (утечка) персональных данных	Веб-сайт	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Средства криптографической защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4

Негативные последствия	Объекты воздействия	Виды воздействия
Нарушение законодательства Российской Федерации (юридическое лицо, индивидуальный предприниматель)	Информационная (автоматизированная) система	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	База данных	ВВ.1; ВВ.2; ВВ.4
	Защищаемая информация	ВВ.1; ВВ.2; ВВ.4
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4
	Объекты файловой системы	ВВ.1; ВВ.2; ВВ.4
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5; ВВ.6
	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	ВВ.2; ВВ.3; ВВ.4; ВВ.6
	Учетные данные пользователя	ВВ.1; ВВ.2; ВВ.4

6. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. Антропогенные источники

6.1.1. В ходе оценки угроз безопасности информации определяются возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие(ая) реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты ИС «Сайт», – актуальные нарушители.

6.1.2. Процесс определения актуальных нарушителей включал:

6.1.2.1. Формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предположений об их отнесении к числу возможных нарушителей (нарушителей, подлежащих дальнейшей оценке), представленных в таблице 9.

Таблица 9 – Перечень рассматриваемых нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
1.	Специальные службы иностранных государств	Нанесение ущерба государству в области обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций; Получение конкурентных преимуществ на уровне государства; Срыв заключения международных договоров; Создание внутриполитического кризиса	Цели не предполагают потенциальное наличие нарушителя
2.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций	Цели не предполагают потенциальное наличие нарушителя
3.	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды; Желание самореализации (подтверждение статуса)	Цели не предполагают потенциальное наличие нарушителя
4.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса)	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
5.	Конкурирующие организации	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ	Цели не предполагают потенциальное наличие нарушителя
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия	Цели не предполагают потенциальное наличие нарушителя
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
8.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
10.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
11.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия;	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

№ п/п	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположения об отнесении к числу возможных нарушителей
		Месть за ранее совершенные действия	
12.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды; Любопытство или желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
13.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

6.1.2.2. Определение характеристик (категория нарушителя и уровень возможности по реализации угроз безопасности информации) возможных нарушителей.

6.1.2.3. Оценка возможности привлечения (вхождения в сговор) одними нарушителями других (в том числе обладающих привилегированными правами доступа).

6.1.2.4. Сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации. По результатам сопоставления определяются актуальные нарушители по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ИС «Сайт» негативным последствиям и соответствующим рискам (видам ущерба).

6.1.3. Итоговые характеристики возможных нарушителей представлены в таблице 10.

Таблица 10 – Характеристики возможных нарушителей

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1.	Отдельные физические лица (хакеры)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
3.	Поставщики вычислительных услуг, услуг связи	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
6.	Авторизованные пользователи систем и сетей	Внутренний	Н1. Нарушитель, обладающий базовыми возможностями	Да
7.	Системные администраторы и администраторы безопасности	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
8.	Бывшие (уволенные) работники (пользователи)	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да

6.1.4. Категория нарушителя определяется исходя из следующих принципов:

– внешний нарушитель – если нарушитель не имеет прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам ИС «Сайт», требующим авторизации;

– внутренний нарушитель – если нарушитель имеет права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам ИС «Сайт». К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ИС «Сайт».

6.1.5. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

6.1.6. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителя по реализации угроз безопасности информации.

6.1.7. Уровень возможности нарушителя определяется исходя из следующих принципов:

– нарушитель, обладающий базовыми возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов;

– нарушитель, обладающий базовыми повышенными возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий средними возможностями по реализации угроз безопасности информации – если нарушитель имеет возможность реализовывать угрозы, в том числе на выявленные им неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей;

– нарушитель, обладающий высокими возможностями по реализации угроз безопасности информации – если имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.

7. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

7.1. В ходе оценки угроз безопасности информации определяются возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в ИС «Сайт», – актуальные способы реализации (возникновения) угроз безопасности информации.

7.2. Процесс определения актуальных способов реализации (возникновения) угроз безопасности информации включал:

7.2.1. Составление перечня рассматриваемых (возможных) способов реализации угроз безопасности. Перечень возможных способов реализации угроз безопасности информации представлен в таблице 11.

Таблица 11 – Перечень возможных способов реализации угроз безопасности информации

Идентификатор	Способы реализации
СР.1	Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей)
СР.2	Внедрение вредоносного программного обеспечения
СР.3	Использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств
СР.4	Установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства
СР.5	Формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных
СР.6	Перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.7	Инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации
СР.8	Нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию)
СР.9	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств
СР.10	Перехват трафика сети передачи данных
СР.11	Несанкционированный физический доступ и (или) воздействие на линии, (каналы) связи, технические средства, машинные носители информации
СР.12	Реализация атак типа "отказ в обслуживании" в отношении технических средств, программного обеспечения и каналов передачи данных

7.2.2. Определение интерфейсов объектов воздействия, определенных в соответствии с разделом 5 настоящей Модели угроз. Интерфейсы объектов воздействия определялись на основе изучения и анализа данных:

– об архитектуре, составе и условиях функционирования ИС «Сайт»;

– о группах пользователей ИС «Сайт», их типов доступа и уровней полномочий.

7.2.3. Определение наличия у актуальных нарушителей возможности доступа к интерфейсам объектов воздействия.

7.2.4. Определение актуальных способов реализации (возникновения) угроз безопасности информации актуальным нарушителем через доступные ему интерфейсы объектов воздействия.

7.3. Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации, включающие описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы актуальными нарушителями, и описание интерфейсов объектов воздействия, доступных для использования актуальным нарушителям, представлены в таблице 12.

Таблица 12 – Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Вид нарушителя	**Категория нарушителя**	**Объекты воздействия**	**Доступные интерфейсы**	**Способы реализации (идентификатор)**
Отдельные физические лица (хакеры)	Внешний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Информационная (автоматизированная) система	Пользователи	СР.1
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
		Защищаемая информация	Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
Поставщики вычислительных услуг, услуг связи	Внутренний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Веб-сайт	Веб-интерфейс системы администрирования Веб-сайта	СР.9
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Веб-сервер	Служебные программы командной строки для управления Веб-сервером	СР.8; СР.9
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Защищаемая информация	Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Информационная (автоматизированная) система	Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4
		Прикладное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Системное программное обеспечение	Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Учетные данные пользователя	Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Защищаемая информация	Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Объекты файловой системы	Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Сетевое оборудование	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Система поддержания температурно-влажностного режима	Консоль управления системой поддержания температурно-влажностного режима	СР.1; СР.9
			Физический доступ к техническим средствам системы поддержания температурно-влажностного режима	СР.1; СР.11
			Удаленные каналы администрирования системы поддержания температурно-влажностного режима	СР.1; СР.9
		Средство вычислительной техники	Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
		Средство защиты информации	Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
Авторизованные пользователи систем и сетей	Внутренний	BIOS/UEFI	Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
		Веб-сайт	Веб-интерфейс пользователя Веб-сайта	СР.1; СР.2
		XML-схема, передаваемая между клиентом и сервером	Каналы связи узлов локальной вычислительной сети	СР.10
		База данных	Прикладное приложение, использующее базу данных	СР.1
		Веб-сервер	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к виртуальным машинам	СР.1; СР.2
			Виртуальные каналы передачи данных	СР.10
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
			Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Системные администраторы и администраторы безопасности	Внутренний	BIOS/UEFI	Консоль управления BIOS/UEFI	СР.1; СР.3; СР.9
			Физический доступ к аппаратному обеспечению BIOS	СР.8; СР.9; СР.11
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Веб-сайт	Веб-интерфейс системы администрирования Веб-сайта	СР.9
		XML-схема, передаваемая между клиентом и сервером	Каналы связи узлов локальной вычислительной сети	СР.10
		База данных	Пользовательский интерфейс СУБД	СР.9
			Служебные программы командной строки СУБД	СР.9
		Веб-сервер	Служебные программы командной строки для управления Веб-сервером	СР.8; СР.9
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения	Каналы связи узлов локальной вычислительной сети	СР.1; СР.10
			Доступ к системе управления виртуальной инфраструктурой	СР.1; СР.8; СР.9
			Доступ к виртуальным машинам	СР.1; СР.2
			Доступ к образам виртуальных машин	СР.1; СР.9
			Доступ к виртуальным устройствам	СР.1; СР.2; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		данных, систему управления виртуальной инфраструктурой)	Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.1; СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ к гипервизору	СР.1; СР.2; СР.8; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к виртуальным устройствам хранения данных и (или) виртуальным дискам	СР.9
			Виртуальные каналы передачи данных	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.7; СР.11
		Информационная (автоматизированная) система	Процесс создания (модернизации) информационной (автоматизированной) системы	СР.4; СР.8; СР.9
			Средства централизованного управления информационной (автоматизированной) системой или ее компонентами	СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.11
			Через функции ввода-вывода низкого уровня (прямого доступа)	СР.8
		Микропрограммное обеспечение	Консоль управления микропрограммным обеспечением	СР.1; СР.3; СР.9
			Механизм обновления микропрограммного обеспечения	СР.2; СР.4

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Объекты файловой системы	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
			Физический доступ к машинным носителям информации	СР.1; СР.4; СР.8; СР.11
		Прикладное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
		Средства криптографической защиты информации	Доступ через средства вычислительной техники	СР.1; СР.9
			Канал удаленного администрирования СКЗИ	СР.1
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевое программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9
		Сетевой трафик	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
			Интерфейсы подключения съемных машинных носителей информации	СР.1; СР.2
		Средство защиты информации	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.9
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
			Каналы удаленного администрирования узла вычислительной сети	СР.1
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.10
			Доступ к объектам файловой системы, содержащим учетные данные пользователя	СР.1; СР.9
Бывшие (уволенные) работники (пользователи)	Внешний	Веб-сайт	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		XML-схема, передаваемая между клиентом и сервером	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Веб-сервер	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
		Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.10
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Объекты файловой системы	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9
		Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Узел вычислительной сети (автоматизированные ра-	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		бочие места, сервера, мар-шрутизаторы, коммутаторы, IoT-устройства и т.п.)		
		Учетные данные пользовате-ля	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10

8. АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

8.1. В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и производится их оценка на актуальность для ИС «Сайт» – актуальные угрозы безопасности информации.

8.2. Процесс определения актуальных угроз безопасности информации включал:

8.2.1. Выделение из исходного перечня угроз безопасности информации возможных угроз по следующему принципу: угроза безопасности информации признается возможной, если имеются нарушитель или иной источник угрозы, объект, на который осуществляется воздействие, способ реализации угрозы безопасности информации, и реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угрозы; негативные последствия]

В качестве исходного перечня угроз безопасности информации использовался банк данных угроз безопасности информации, сформированный ФСТЭК России (http://bdu.fstec.ru/).

Перечень исключенных из исходного перечня угроз безопасности информации представлен в Приложении № 4.

8.2.2. Оценку возможных угроз на предмет актуальности по следующему принципу: угроза признается актуальной, если имеется хотя бы один сценарий реализации угрозы безопасности информации.

Сценарии определяются для соответствующих способов реализации угроз безопасности информации.

Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации представлен в Приложении № 5.

8.3. По результатам оценки возможных угроз безопасности выявлено актуальных угроз: 133. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 13.

Таблица 13 – Актуальные угрозы безопасности информации

Идентификатор угрозы	**Наименование угрозы**
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации

Идентификатор угрозы	Наименование угрозы
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.033	Угроза использования слабостей кодирования входных данных
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.041	Угроза межсайтового скриптинга
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи

Идентификатор угрозы	Наименование угрозы
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.088	Угроза несанкционированного копирования защищаемой информации
УБИ.089	Угроза несанкционированного редактирования реестра
УБИ.090	Угроза несанкционированного создания учётной записи пользователя
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.093	Угроза несанкционированного управления буфером
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.103	Угроза определения типов объектов защиты
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.108	Угроза ошибки обновления гипервизора
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники

Идентификатор угрозы	Наименование угрозы
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.119	Угроза перехвата управления гипервизором
УБИ.120	Угроза перехвата управления средой виртуализации
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.128	Угроза подмены доверенного пользователя
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.156	Угроза утраты носителей информации
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.158	Угроза форматирования носителей информации
УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.162	Угроза эксплуатации цифровой подписи программного кода
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.169	Угроза наличия механизмов разработчика
УБИ.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.172	Угроза распространения «почтовых червей»

Идентификатор угрозы	Наименование угрозы
УБИ.173	Угроза «спама» веб-сервера
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
УБИ.179	Угроза несанкционированной модификации защищаемой информации
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
УБИ.182	Угроза физического устаревания аппаратных компонентов
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза перехвата управления информационной системой
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

9. ОЦЕНКА УГРОЗ В СООТВЕТСТВИИ С МЕТОДИЧЕСКИМИ ДОКУМЕНТАМИ ФСБ РОССИИ

9.1. На основании исходных данных об объектах защиты (в соответствии с разделом 5 настоящей Модели угроз) и источниках атак (в соответствии с разделом 6.1 настоящей Модели угроз) ИС «Сайт» определены обобщенные возможности источников атак (таблица 14).

Таблица 14 – Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Предположение о возможности источников атак
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

9.2. В соответствии с нормативно-правовыми документами ФСБ России реализация угроз безопасности информации определяется возможностями источников атак.

9.3. Исходя из обобщенных возможностей источников атак определены уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы). Результаты приведены в Приложении № 7.

9.4. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КС3.

Источники разработки модели угроз

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

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– 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 Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методический документ «Методика оценки угроз безопасности информации», утвержденный Федеральной службы по техническому и экспортному контролю 5 февраля 2021 г.;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю 15 февраля 2008 г.;

– 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;

– 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 29099-91 «Сети вычислительные локальные. Термины и определения», утвержденный постановлением Комитета стандартизации и метрологии СССР от 25 сентября 1991 г. № 1491;

– ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1520-ст;

– ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», утвержденный приказом Росстандарта от 19 ноября 2021 г. № 1521-ст;

– ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утвержденный постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 г. № 3469;

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», утвержденный постановлением Госстандарта России от 9 февраля 1995 г. № 49;

– 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 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», утвержденный постановлением Госстандарта России от 14 июля 1998 г. № 295;

– 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 2.105-2019 «Единая система конструкторской документации. Общие требования к текстовым документам», утвержденный приказом Росстандарта от 29 апреля 2019 г. № 175-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 Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов», утвержденный приказом Росстандарта от 25 октября 2021 г. № 1297-ст;

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

ПРИЛОЖЕНИЕ № 2

Соответствие возможных целей реализации угроз безопасности информации с негативными последствиями

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
1.	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.5	НП.8	–
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	НП.5	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7	–
3.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	–	НП.8	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.8	–
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Получение конкурентных преимуществ	–	НП.8	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.8	–
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.5	НП.6; НП.7; НП.8	–
6.	Авторизованные пользователи систем и сетей	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.3; НП.5	НП.8	–

№ п/п	Вид нарушителя	Цели реализации угроз безопасности информации	Вид риска (ущерба)		
			Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.5	НП.6; НП.7; НП.8	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–
7.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Любопытство или желание самореализации (подтверждение статуса)	НП.1; НП.5	НП.8	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.3; НП.5	НП.6; НП.7; НП.8	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–
8.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды	НП.5	–	–
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.5	–	–

Уровни возможностей нарушителя

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
Н1	Нарушитель, обладающий базовыми возможностями	– Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. – Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. – Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним
Н2	Нарушитель, обладающий базовыми повышенными возможностями	– Обладает всеми возможностями нарушителей с базовыми возможностями. – Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. – Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. – Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. – Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах
Н3	Нарушитель, обладающий средними возможностями	– Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. – Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). – Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств.

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности
		– Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. – Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. – Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. – Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц
Н4	Нарушитель, обладающий высокими возможностями	– Обладает всеми возможностями нарушителей со средними возможностями. – Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». – Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. – Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. – Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. – Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. – Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. – Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей

Перечень исключенных из базового перечня угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе	Отсутствуют объекты воздействия
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе	Отсутствуют объекты воздействия
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Отсутствуют объекты воздействия
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies	Отсутствуют объекты воздействия
УБИ.020	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	Отсутствуют объекты воздействия
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг	Отсутствуют объекты воздействия
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.026	Угроза искажения XML-схемы	Отсутствуют условия, при которых может быть реализована угроза
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Отсутствуют объекты воздействия
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.038	Угроза исчерпания вычислительных ресурсов хранилища больших данных	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.040	Угроза конфликта юрисдикций различных стран	Отсутствуют объекты воздействия
УБИ.042	Угроза межсайтовой подделки запроса	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.043	Угроза нарушения доступности облачного сервера	Отсутствуют объекты воздействия
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Отсутствуют объекты воздействия
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Отсутствуют объекты воздействия
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	Отсутствуют объекты воздействия
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Отсутствуют объекты воздействия
УБИ.055	Угроза незащищённого администрирования облачных услуг	Отсутствуют объекты воздействия
УБИ.056	Угроза некачественного переноса инфраструктуры в облако	Отсутствуют объекты воздействия
УБИ.057	Угроза неконтролируемого копирования данных внутри хранилища больших данных	Отсутствуют объекты воздействия
УБИ.058	Угроза неконтролируемого роста числа виртуальных машин	Отсутствуют объекты воздействия
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке	Отсутствуют объекты воздействия
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке	Отсутствуют объекты воздействия
УБИ.066	Угроза неопределённости ответственности за обеспечение безопасности облака	Отсутствуют объекты воздействия
УБИ.070	Угроза непрерывной модернизации облачной инфраструктуры	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.081	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	Отсутствуют объекты воздействия
УБИ.082	Угроза несанкционированного доступа к сегментам вычислительного поля	Отсутствуют объекты воздействия
УБИ.083	Угроза несанкционированного доступа к системе по беспроводным каналам	Отсутствуют объекты воздействия
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Отсутствуют объекты воздействия
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.097	Угроза несогласованности правил доступа к большим данным	Отсутствуют объекты воздействия
УБИ.101	Угроза общедоступности облачной инфраструктуры	Отсутствуют объекты воздействия
УБИ.105	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.106	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	Отсутствуют объекты воздействия
УБИ.107	Угроза отключения контрольных датчиков	Отсутствуют объекты воздействия
УБИ.110	Угроза перегрузки грид-системы вычислительными заданиями	Отсутствуют объекты воздействия
УБИ.112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Отсутствуют объекты воздействия
УБИ.125	Угроза подключения к беспроводной сети в обход процедуры аутентификации	Отсутствуют объекты воздействия
УБИ.126	Угроза подмены беспроводного клиента или точки доступа	Отсутствуют объекты воздействия
УБИ.127	Угроза подмены действия пользователя путём обмана	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.131	Угроза подмены субъекта сетевого доступа	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.132	Угроза получения предварительной информации об объекте защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.133	Угроза получения сведений о владельце беспроводного устройства	Отсутствуют объекты воздействия
УБИ.134	Угроза потери доверия к поставщику облачных услуг	Отсутствуют объекты воздействия
УБИ.135	Угроза потери и утечки данных, обрабатываемых в облаке	Отсутствуют условия, при которых может быть реализована угроза
УБИ.136	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	Отсутствуют объекты воздействия
УБИ.137	Угроза потери управления облачными ресурсами	Отсутствуют объекты воздействия
УБИ.138	Угроза потери управления собственной инфраструктурой при переносе её в облако	Отсутствуют объекты воздействия
УБИ.139	Угроза преодоления физической защиты	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.141	Угроза привязки к поставщику облачных услуг	Отсутствуют объекты воздействия
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев	Отсутствуют объекты воздействия
УБИ.146	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	Отсутствуют объекты воздействия
УБИ.147	Угроза распространения несанкционированно повышенных прав на всю грид-систему	Отсутствуют объекты воздействия
УБИ.148	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	Отсутствуют объекты воздействия
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Отсутствуют объекты воздействия
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Отсутствуют объекты воздействия
УБИ.181	Угроза перехвата одноразовых паролей в режиме реального времени	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Отсутствуют объекты воздействия
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Отсутствуют объекты воздействия
УБИ.189	Угроза маскирования действий вредоносного кода	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.194	Угроза несанкционированного использования привилегированных функций мобильного устройства	Отсутствуют объекты воздействия
УБИ.195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	Отсутствуют объекты воздействия
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie	Отсутствуют объекты воздействия
УБИ.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	Отсутствуют объекты воздействия
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Отсутствуют объекты воздействия
УБИ.206	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	Отсутствуют объекты воздействия
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Отсутствуют объекты воздействия
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.213	Угроза обхода многофакторной аутентификации	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Уровень возможностей нарушителей недостаточен для реализации угрозы
УБИ.216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Отсутствуют объекты воздействия
УБИ.218	Угроза раскрытия информации о модели машинного обучения	Отсутствуют объекты воздействия
УБИ.219	Угроза хищения обучающих данных	Отсутствуют объекты воздействия
УБИ.220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Отсутствуют объекты воздействия
УБИ.221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Отсутствуют объекты воздействия
УБИ.222	Угроза подмены модели машинного обучения	Отсутствуют объекты воздействия

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях	Т1.1 Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2 Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.3 Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4 Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
		Т1.5 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств
		Т1.6 Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора
		Т1.7 Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		Т1.8 Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		Т1.9 Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей.
		Т1.10 Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)

№	Тактика	Основные техники
		T1.11 Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		T1.12 Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		T1.13 Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		T1.14 Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		T1.15 Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках
		T1.16 Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров
		T1.17 Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.18 Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.19 Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.20 Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.21 Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем анализа и обобщения информации перехватываемой в сети передачи информации

№	Тактика	Основные техники
		Т1.22 Поиск и покупка специализированного программного обеспечения (вредоносного кода) на специализированных нелегальных площадках
Т2	Получение первоначального доступа к компонентам систем и сетей	Т2.1 Использование внешних сервисов организации в сетях публичного доступа (Интернет)
		Т2.2 Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра
		Т2.3 Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.4 Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.5 Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке
		Т2.6 Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
		Т2.7 Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций
		Т2.8 Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.9 Несанкционированное подключение внешних устройств
		Т2.10 Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
		Т2.11 Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
		Т2.12 Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа
		Т2.13 Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки
		Т2.14 Доступ путем эксплуатации недостатков систем биометрической аутентификации

№	Тактика	Основные техники
		Т2.15 Доступ путем использования недостатков правовых норм других стран, участвующих в трансграничной передаче облачного трафика
		Т2.16 Доступ путем использования возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1 Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.2 Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
		Т3.3 Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
		Т3.4 Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
		Т3.5 Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
		Т3.6 Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
		Т3.7 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т3.8 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т3.9 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т3.10 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т3.11 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами

№	Тактика	Основные техники
		Т3.12 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.13 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.14 Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		Т3.15 Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
		Т3.16 Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL
		Т3.17 Планирование запуска вредоносного кода при запуске компьютера путем эксплуатации стандартных механизмов BIOS (UEFI) и т.п.
		Т3.18 Эксплуатация уязвимостей типа локальное исполнение программного кода
Т4	Закрепление (сохранение доступа) в системе или сети	Т4.1 Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2 Использование штатных средств удаленного доступа и управления операционной системы
		Т4.3 Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода
		Т4.4 Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
		Т4.5 Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети

№	Тактика	Основные техники
		Т4.6 Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
		Т4.7 Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей
		Т4.8 Использование прошивок устройств с уязвимостями, к примеру, внедрение новых функций в BIOS (UEFI)
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1 Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		Т5.2 Использование штатных средств удаленного доступа и управления операционной системы
		Т5.3 Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т5.4 Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т5.5 Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т5.6 Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения
		Т5.7 Туннелирование трафика управления через VPN
		Т5.8 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т5.9 Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
		Т5.10 Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
		Т5.11 Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		Т5.12 Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.

№	Тактика	Основные техники
		Т5.13 Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения
Т6	Повышение привилегий по доступу к компонентам систем и сетей	Т6.1 Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
		Т6.2 Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий
		Т6.4 Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи)
		Т6.5 Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций
		Т6.6 Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима
		Т6.7 Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями
		Т6.8 Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей
		Т6.9 Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Т7.1 Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения
		Т7.2 Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3 Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4 Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов

№	Тактика	Основные техники
		Т7.5 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
		Т7.6 Подделка данных вывода средств защиты от угроз информационной безопасности
		Т7.7 Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
		Т7.8 Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки
		Т7.9 Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей
		Т7.10 Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
		Т7.11 Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе
		Т7.12 Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности
		Т7.13 Создание скрытых файлов, скрытых учетных записей
		Т7.14 Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
		Т7.15 Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
		Т7.16 Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки
		Т7.17 Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети

№	Тактика	Основные техники
		Т7.18 Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе
		Т7.19 Туннелирование трафика управления через VPN
		Т7.20 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т7.21 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22 Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23 Подмена файлов легитимных программ и библиотек непосредственно в системе
		Т7.24 Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи
		Т7.25 Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями
		Т7.26 Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
		Т7.27 Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28 Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т7.29 Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы

№	Тактика	Основные техники
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1 Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
		Т8.2 Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
		Т8.3 Использование механизмов дистанционной установки программного обеспечения и конфигурирования
		Т8.4 Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям
		Т8.5 Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т8.6 Копирование вредоносного кода на съемные носители
		Т8.7 Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
		Т8.8 Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1 Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
		Т9.2 Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		Т9.3 Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т9.4 Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т9.5 Отправка данных по известным протоколам управления и передачи данных
		Т9.6 Отправка данных по собственным протоколам
		Т9.7 Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения
		Т9.8 Туннелирование трафика передачи данных через VPN
		Т9.9 Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие

№	Тактика	Основные техники
		Т9.10 Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т9.11 Отправка данных через альтернативную среду передачи данных
		Т9.12 Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации
		Т9.13 Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
		Т9.14 Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1 Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		Т10.2 Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		Т10.3 Несанкционированное воздействие на программные модули прикладного программного обеспечения
		Т10.4 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
		Т10.5 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения
		Т10.6 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства
		Т10.7 Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
		Т10.8 Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
		Т10.9 Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.10 Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
		Т10.11 Нецелевое использование ресурсов системы
		Т10.12 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов,

№	Тактика	Основные техники
		объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.13 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.14 Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.15 Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой

Результаты оценки возможных угроз безопасности информации

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средства криптографической защиты информации	НП.5	СР.1; СР.8	Сценарий реализации УБИ.003: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т10 (Т10.2; Т10.5)
УБИ.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.9; СР.11	Сценарий реализации УБИ.004: – Т1 (Т1.9; Т1.15; Т1.16); – Т2 (Т2.9)
УБИ.006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.006: – Т1 (Т1.4; Т1.5); – Т2 (Т2.5; Т2.10); – Т3 (Т3.1; Т3.2; Т3.15); – Т4 (Т4.2); – Т5 (Т5.2)
УБИ.007	Угроза воздействия на прог-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное	НП.1; НП.5; НП.8	СР.1; СР.3; СР.9	Сценарий реализации УБИ.007: – Т1 (Т1.9; Т1.16); – Т2 (Т2.6);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	раммы с высокими привилегиями		обеспечение, Системное программное обеспечение			– Т3 (Т3.5); – Т6 (Т6.2; Т6.3)
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.008: – Т1 (Т1.6); – Т2 (Т2.10); – Т4 (Т4.1)
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.8; СР.9	Сценарий реализации УБИ.009: – Т1 (Т1.9); – Т3 (Т3.18); – Т4 (Т4.8)
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.2	Сценарий реализации УБИ.010: – Т1 (Т1.5; Т1.9; Т1.16; Т1.22); – Т2 (Т2.5; Т2.6); – Т3 (Т3.1; Т3.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Объекты файловой системы, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.3; СР.9	Сценарий реализации УБИ.012: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5; Т2.6); – Т3 (Т3.7)
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.9	Сценарий реализации УБИ.013: – Т1 (Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1; СР.3; СР.9	Сценарий реализации УБИ.014: – Т1 (Т1.5; Т1.16; Т1.19); – Т2 (Т2.5; Т2.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.5; НП.8	СР.1; СР.3	Сценарий реализации УБИ.015: – Т1 (Т1.9; Т1.16); – Т2 (Т2.3; Т2.5; Т2.6); – Т6 (Т6.3; Т6.6)
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.8	Сценарий реализации УБИ.018: – Т2 (Т2.5); – Т10 (Т10.2)
УБИ.019	Угроза заражения DNS-кеша	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1	Сценарий реализации УБИ.019: – Т8 (Т8.8)
УБИ.022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение		СР.2; СР.4	Сценарий реализации УБИ.022: – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.2; Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.5; НП.8	СР.1; СР.4	Сценарий реализации УБИ.023: – Т2 (Т2.7); – Т3 (Т3.7); – Т10 (Т10.3)
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.3	Сценарий реализации УБИ.025: – Т10 (Т10.2; Т10.4)
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.2; СР.3	Сценарий реализации УБИ.027: – Т3 (Т3.2); – Т8 (Т8.1)
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы	НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.028: – Т1 (Т1.5; Т1.9); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации	НП.1; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.030: – Т1 (Т1.1; Т1.9; Т1.16); – Т2 (Т2.4)
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.8	Сценарий реализации УБИ.031: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.4; Т2.5); – Т6 (Т6.3; Т6.6)
УБИ.033	Угроза использования слабостей кодирования входных данных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.033: – Т1 (Т1.5); – Т2 (Т2.5; Т2.6); – Т10 (Т10.2)
УБИ.034	Угроза использования слабостей про-	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Сетевое программное обеспечение, Сетевой трафик, Системное	НП.4; НП.5; НП.8	СР.1; СР.3	Сценарий реализации УБИ.034: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	токолов сетевого/локального обмена данными	Внутренний нарушитель, обладающий базовыми повышенными возможностями	программное обеспечение			– Т10 (Т10.1)
УБИ.036	Угроза исследования механизмов работы программы	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.8	Сценарий реализации УБИ.036: – Т2 (Т2.5)
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.037: – Т1 (Т1.9); – Т2 (Т2.5; Т2.6)
УБИ.041	Угроза межсайтового скриптинга	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.041: – Т1 (Т1.1; Т1.5; Т1.8); – Т2 (Т2.1); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.2	Сценарий реализации УБИ.044: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.3; Т2.5); – Т3 (Т3.1); – Т10 (Т10.2; Т10.3)
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1	Сценарий реализации УБИ.045: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5); – Т4 (Т4.6); – Т10 (Т10.2; Т10.6)
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и		СР.1; СР.9	Сценарий реализации УБИ.046: – Т2 (Т2.4; Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.8	Сценарий реализации УБИ.048: – Т2 (Т2.3; Т2.5); – Т3 (Т3.7); – Т4 (Т4.3; Т4.5; Т4.7); – Т10 (Т10.2; Т10.7)
УБИ.049	Угроза нарушения целостности данных кеша	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение		СР.1; СР.9	Сценарий реализации УБИ.049: – Т2 (Т2.5); – Т3 (Т3.9); – Т10 (Т10.1; Т10.2)
УБИ.051	Угроза невозможности восстановления	Внутренний нарушитель, обладающий базовыми возможностями,	Узел вычислительной сети (автоматизиро-	НП.1; НП.5; НП.8	СР.9	Сценарий реализации УБИ.051: – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель, обладающий базовыми повышенными возможностями	ванные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.11	Сценарий реализации УБИ.053: – Т2 (Т2.5)
УБИ.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.8; СР.9	Сценарий реализации УБИ.059: – Т10 (Т10.10)
УБИ.061	Угроза некорректного за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	База данных, Сетевое программное обеспечение, Сетевой трафик	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8	СР.1; СР.9	Сценарий реализации УБИ.061: – Т1 (Т1.5); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	дания структуры данных транзакции					
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение		СР.1; СР.2; СР.9	Сценарий реализации УБИ.062: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.063: – Т2 (Т2.5); – Т10 (Т10.11)
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.067: – Т1 (Т1.13; Т1.14); – Т10 (Т10.1)
УБИ.068	Угроза неправомерного/некорректного использования интерфейса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.068: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	взаимодействия с приложением		программное обеспечение, Системное программное обеспечение			
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.069: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.071: – Т1 (Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.072: – Т2 (Т2.5); – Т3 (Т3.8; Т3.18); – Т4 (Т4.6)
УБИ.073	Угроза несанкционированного доступа к активному и	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-		СР.1; СР.2; СР.9	Сценарий реализации УБИ.073: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	(или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети		шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой), Микропрограммное обеспечение, Сетевое оборудование, Сетевое программное обеспечение			
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.074: – Т1 (Т1.12); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.075	Угроза несанкционированного доступа к виртуальным	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-		СР.1; СР.9	Сценарий реализации УБИ.075: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	каналам передачи	Внутренний нарушитель, обладающий базовыми повышенными возможностями	шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.9	Сценарий реализации УБИ.076: – Т10 (Т10.10)
УБИ.077	Угроза несанкционированного доступа к данным за пределами за-	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы вирту-		СР.1; СР.2	Сценарий реализации УБИ.077: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.1); – Т4 (Т4.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	резервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение		альных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			– Т7 (Т7.18); – Т10 (Т10.1; Т10.11)
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.8; СР.9	Сценарий реализации УБИ.078: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства,		СР.1; СР.8	Сценарий реализации УБИ.079: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5); – Т10 (Т10.1; Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	стороны других виртуальных машин		виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.8	Сценарий реализации УБИ.080: – Т1 (Т1.5; Т1.16); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и		СР.1; СР.9	Сценарий реализации УБИ.084: – Т1 (Т1.5; Т1.22)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8	СР.1; СР.8	Сценарий реализации УБИ.085: – Т1 (Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Учетные данные пользователя	НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.086: – Т1 (Т1.5; Т1.12; Т1.22); – Т2 (Т2.4; Т2.11); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.9	Сценарий реализации УБИ.087: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.088	Угроза несанкционированного копирования защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8	СР.1	Сценарий реализации УБИ.088: – Т2 (Т2.4; Т2.9); – Т10 (Т10.1)
УБИ.089	Угроза несанкционированного редактирования реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение		СР.1; СР.8	Сценарий реализации УБИ.089: – Т1 (Т1.5; Т1.9); – Т2 (Т2.4); – Т4 (Т4.5); – Т10 (Т10.1)
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение		СР.1; СР.8	Сценарий реализации УБИ.090: – Т1 (Т1.5); – Т2 (Т2.4); – Т4 (Т4.1); – Т5 (Т5.2); – Т10 (Т10.2)
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники, Объекты файловой системы	НП.2; НП.3; НП.4; НП.5; НП.7; НП.8	СР.1; СР.8	Сценарий реализации УБИ.091: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.093: – Т1 (Т1.9); – Т2 (Т2.4; Т2.5); – Т3 (Т3.2); – Т10 (Т10.1)
УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.094: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.1; Т10.3)
УБИ.095	Угроза несанкционированного управления указателями	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.095: – Т1 (Т1.5); – Т2 (Т2.4; Т2.11); – Т3 (Т3.2); – Т10 (Т10.3; Т10.4)
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы,	НП.1; НП.4; НП.5; НП.8	СР.1	Сценарий реализации УБИ.098: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			коммутаторы, IoT-устройства и т.п.)			
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.099: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.8; СР.9	Сценарий реализации УБИ.100: – Т2 (Т2.4; Т2.5); – Т4 (Т4.1); – Т6 (Т6.6)
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.102: – Т2 (Т2.5)
УБИ.103	Угроза определения типов	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой	НП.1; НП.4; НП.5; НП.8	СР.8; СР.9	Сценарий реализации УБИ.103: – Т1 (Т1.1; Т1.3);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	объектов защиты		трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			– Т2 (Т2.4)
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1	Сценарий реализации УБИ.104: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3)
УБИ.108	Угроза ошибки обновления гипервизора	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной		СР.1; СР.9	Сценарий реализации УБИ.108: – Т2 (Т2.5); – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			инфраструктурой)			
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.109: – Т2 (Т2.5; Т2.6); – Т10 (Т10.10)
УБИ.111	Угроза передачи данных по скрытым каналам	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевой трафик, Системное программное обеспечение	НП.4; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.111: – Т2 (Т2.4); – Т9 (Т9.10)
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.5; НП.8	СР.1	Сценарий реализации УБИ.113: – Т2 (Т2.5; Т2.11); – Т10 (Т10.8)
УБИ.114	Угроза переполнения целочисленных переменных	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.114: – Т1 (Т1.1; Т1.5; Т1.9); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.115	Угроза перехвата вводимой	Внешний нарушитель, обладающий базовыми возможностями,	Прикладное программное обеспечение,	НП.1; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.115:

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	и выводимой на периферийные устройства информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение			– Т1 (Т1.4; Т1.12); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т10 (Т10.1; Т10.3)
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.4; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.116: – Т1 (Т1.3); – Т2 (Т2.4; Т2.5; Т2.11)
УБИ.117	Угроза перехвата привилегированного потока	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.117: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т6 (Т6.1); – Т10 (Т10.1)
УБИ.118	Угроза перехвата привилегированного процесса	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.118: – Т1 (Т1.5); – Т2 (Т2.4; Т2.5; Т2.11); – Т3 (Т3.1); – Т4 (Т4.1); – Т6 (Т6.3)
УБИ.119	Угроза перехвата управления гипервизором	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные ма-		СР.1; СР.8	Сценарий реализации УБИ.119: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			шины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)			
УБИ.120	Угроза перехвата управления средой виртуализации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Виртуальная инфраструктура (воздействие на гипервизор, виртуальные машины, образы виртуальных машин, виртуальные устройства, виртуальные диски и виртуальные устройства хранения данных, систему управления виртуальной инфраструктурой)		СР.1; СР.8	Сценарий реализации УБИ.120: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.1)
УБИ.121	Угроза повреждения системного реестра	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.121: – Т2 (Т2.4; Т2.5; Т2.11); – Т10 (Т10.8; Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
		Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.122	Угроза повышения привилегий	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Системное программное обеспечение		СР.1; СР.2; СР.8	Сценарий реализации УБИ.122: – Т2 (Т2.5); – Т3 (Т3.5); – Т6 (Т6.1); – Т10 (Т10.3)
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.8	Сценарий реализации УБИ.123: – Т1 (Т1.6); – Т2 (Т2.5; Т2.10); – Т4 (Т4.1); – Т10 (Т10.1)
УБИ.124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение, Средство защиты информации	НП.1; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.124: – Т1 (Т1.22); – Т2 (Т2.5; Т2.11); – Т7 (Т7.6)
УБИ.128	Угроза подмены доверенного пользователя	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.128: – Т1 (Т1.5); – Т2 (Т2.5; Т2.9)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
			рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.8	Сценарий реализации УБИ.129: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.7); – Т4 (Т4.6; Т4.7)
УБИ.130	Угроза подмены содержимого сетевых ресурсов	Внешний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Сетевой трафик	НП.1; НП.4; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.130: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.2)
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1; СР.9; СР.12	Сценарий реализации УБИ.140: – Т2 (Т2.3; Т2.5); – Т10 (Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Микропрограммное обеспечение, Сетевое оборудование	НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.143: – Т1 (Т1.5); – Т2 (Т2.5); – Т7 (Т7.8); – Т10 (Т10.10)
УБИ.144	Угроза программного сброса пароля BIOS	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1	Сценарий реализации УБИ.144: – Т1 (Т1.9; Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.6)
УБИ.145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.145: – Т2 (Т2.4; Т2.5; Т2.8); – Т3 (Т3.3)
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Объекты файловой системы, Системное программное обеспечение	НП.5; НП.8	СР.1; СР.4	Сценарий реализации УБИ.149: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.10)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.9	Сценарий реализации УБИ.150: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Внешний нарушитель, обладающий базовыми возможностями	Веб-сервер		СР.1; СР.9	Сценарий реализации УБИ.151: – Т1 (Т1.5; Т1.22); – Т2 (Т2.3; Т2.5)
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Системное программное обеспечение, Учетные данные пользователя	НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.152: – Т1 (Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.10)
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.153: – Т1 (Т1.2; Т1.22); – Т2 (Т2.3; Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внутренний нарушитель, обладающий базовыми повышенными возможностями	BIOS/UEFI		СР.1; СР.9	Сценарий реализации УБИ.154: – Т1 (Т1.5); – Т2 (Т2.5); – Т3 (Т3.8); – Т4 (Т4.6); – Т7 (Т7.22); – Т10 (Т10.6; Т10.10)
УБИ.155	Угроза утраты вычислительных ресурсов	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое программное обеспечение, Сетевой трафик, Системное программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.155: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5; Т2.11); – Т10 (Т10.10)
УБИ.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8	СР.1; СР.8; СР.9	Сценарий реализации УБИ.156: – Т1 (Т1.10); – Т10 (Т10.1; Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий базовыми возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8	СР.1; СР.9; СР.11	Сценарий реализации УБИ.157: – Т2 (Т2.2); – Т10 (Т10.8; Т10.10)
УБИ.158	Угроза форматирования носителей информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.158: – Т2 (Т2.2; Т2.5); – Т10 (Т10.8)
УБИ.159	Угроза «форсированного веб-браузинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8	СР.1	Сценарий реализации УБИ.159: – Т2 (Т2.1; Т2.5); – Т10 (Т10.1)
УБИ.160	Угроза хищения средств хранения, обработки и (или)	Внешний нарушитель, обладающий базовыми возможностями	Машинный носитель информации в составе средств вычислительной техники, Сетевое	НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.160: – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ввода/вывода/передачи информации		оборудование, Средство вычислительной техники			
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.4	Сценарий реализации УБИ.162: – Т1 (Т1.10); – Т3 (Т3.11; Т3.16)
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение		СР.1; СР.9	Сценарий реализации УБИ.163: – Т1 (Т1.3); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6	СР.9	Сценарий реализации УБИ.165: – Т2 (Т2.5)
УБИ.166	Угроза внедрения системной избыточности	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6	СР.9	Сценарий реализации УБИ.166: – Т2 (Т2.5)
УБИ.167	Угроза заражения компьюте-	Внутренний нарушитель, обладающий базовыми возможностями,	Узел вычислительной сети (автоматизированные рабочие мес-	НП.1; НП.5; НП.8	СР.2; СР.8	Сценарий реализации УБИ.167: – Т2 (Т2.4); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ра при посещении неблагонадёжных сайтов	Внутренний нарушитель, обладающий базовыми повышенными возможностями	та, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)			
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Учетные данные пользователя	НП.5; НП.8	СР.1	Сценарий реализации УБИ.168: – Т4 (Т4.1)
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.169: – Т2 (Т2.5; Т2.6); – Т3 (Т3.12)
УБИ.170	Угроза неправомерного шифрования информации	Внешний нарушитель, обладающий базовыми возможностями	Объекты файловой системы	НП.5; НП.8	СР.4	Сценарий реализации УБИ.170: – Т2 (Т2.4); – Т3 (Т3.3); – Т10 (Т10.8)
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Внешний нарушитель, обладающий базовыми возможностями	Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.5; НП.8	СР.2; СР.8	Сценарий реализации УБИ.171: – Т1 (Т1.2); – Т2 (Т2.3; Т2.4; Т2.5); – Т3 (Т3.1); – Т4 (Т4.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.172	Угроза распространения «почтовых червей»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение		СР.1; СР.2; СР.8	Сценарий реализации УБИ.172: – Т1 (Т1.1); – Т2 (Т2.3)
УБИ.173	Угроза «спама» веб-сервера	Внешний нарушитель, обладающий базовыми возможностями	Веб-сервер		СР.1	Сценарий реализации УБИ.173: – Т1 (Т1.1); – Т2 (Т2.1)
УБИ.174	Угроза «фарминга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.174: – Т1 (Т1.1; Т1.8); – Т3 (Т3.3)
УБИ.175	Угроза «фишинга»	Внешний нарушитель, обладающий базовыми возможностями	Сетевое программное обеспечение, Сетевой трафик, Узел вычислительной сети (автоматизированные рабочие места, сервера, маршрутизаторы, коммутаторы, IoT-устройства и т.п.)	НП.1; НП.4; НП.5; НП.8	СР.1	Сценарий реализации УБИ.175: – Т1 (Т1.1; Т1.11); – Т2 (Т2.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Внешний нарушитель, обладающий базовыми возможностями	Средство защиты информации		СР.1; СР.8; СР.12	Сценарий реализации УБИ.176: – Т10 (Т10.3; Т10.10)
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.177: – Т10 (Т10.14)
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение		СР.1; СР.3	Сценарий реализации УБИ.178: – Т2 (Т2.4; Т2.5); – Т10 (Т10.5)
УБИ.179	Угроза несанкционированной модифи-	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями,	Объекты файловой системы	НП.5; НП.8	СР.8; СР.11	Сценарий реализации УБИ.179: – Т2 (Т2.5); – Т10 (Т10.7; Т10.8)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	кации защищаемой информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Система поддержания температурно-влажностного режима		СР.1; СР.9	Сценарий реализации УБИ.180: – Т10 (Т10.14)
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.182: – Т10 (Т10.8; Т10.10)
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации		СР.1; СР.9	Сценарий реализации УБИ.185: – Т2 (Т2.4); – Т7 (Т7.4)
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое программное обеспечение		СР.1; СР.2; СР.8	Сценарий реализации УБИ.186: – Т1 (Т1.1); – Т3 (Т3.3)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство защиты информации		СР.1; СР.8; СР.9	Сценарий реализации УБИ.187: – Т2 (Т2.4); – Т7 (Т7.4); – Т10 (Т10.2)
УБИ.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.2; СР.9	Сценарий реализации УБИ.188: – Т2 (Т2.7); – Т3 (Т3.7; Т3.8; Т3.10); – Т7 (Т7.24); – Т10 (Т10.7)
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.2; СР.8; СР.9	Сценарий реализации УБИ.191: – Т3 (Т3.2)
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.9	Сценарий реализации УБИ.192: – Т2 (Т2.5); – Т10 (Т10.2)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Сетевое оборудование, Средство вычислительной техники	НП.5; НП.8	СР.1; СР.2; СР.8	Сценарий реализации УБИ.203: – Т2 (Т2.5); – Т3 (Т3.2); – Т6 (Т6.3); – Т9 (Т9.11)
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель, обладающий базовыми возможностями	Средство вычислительной техники	НП.5; НП.8	СР.1; СР.8	Сценарий реализации УБИ.205: – Т2 (Т2.4)
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Средство вычислительной техники	НП.5; НП.8	СР.2; СР.8	Сценарий реализации УБИ.208: – Т10 (Т10.11)
УБИ.209	Угроза несанкционированного доступа к	Внешний нарушитель, обладающий базовыми возможностями,	Средство вычислительной техники	НП.5; НП.8	СР.1	Сценарий реализации УБИ.209: – Т10 (Т10.1; Т10.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	защищаемой памяти ядра процессора	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями				
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Внутренний нарушитель, обладающий базовыми возможностями, Внутренний нарушитель, обладающий базовыми повышенными возможностями	Системное программное обеспечение		СР.1; СР.9	Сценарий реализации УБИ.211: – Т10 (Т10.2)
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система, Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.5; НП.6; НП.8	СР.1	Сценарий реализации УБИ.212: – Т2 (Т2.4; Т2.5); – Т8 (Т8.1); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Информационная (автоматизированная) система	НП.1; НП.6	СР.1; СР.8	Сценарий реализации УБИ.214: – Т7 (Т7.4)
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Микропрограммное обеспечение, Прикладное программное обеспечение, Сетевое программное обеспечение, Системное программное обеспечение	НП.1; НП.5; НП.8	СР.1; СР.2	Сценарий реализации УБИ.217: – Т3 (Т3.8); – Т7 (Т7.24)

Уточненные возможности нарушителей и направления атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИС «Сайт», не имеют возможности находиться в помещениях, где расположена ИС «Сайт», в отсутствие пользователей ИС «Сайт»; – Работа пользователей ИС «Сайт» регламентирована; – Ответственный за обеспечение безопасности ПДн, администраторы ИС «Сайт» назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС «Сайт», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Проводится обучение пользователей ИС «Сайт» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ	Да	– Ответственный пользователь криптосредств назначается не из числа особо доверенных лиц; – Документация на СКЗИ не хранится у ответственного пользователя криптосредств в металлическом сейфе (шкафу); – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ	Нет	– Работа пользователей ИС «Сайт» регламентирована; – Проводится обучение пользователей ИС «Сайт» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Сведения о физических мерах защиты объектов, в которых размещена ИС «Сайт», доступны ограниченному кругу сотрудников
1.4	Использование штатных средств ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	Да	– Работа пользователей ИС «Сайт» регламентирована; – Ответственный за обеспечение безопасности ПДн, администраторы ИС «Сайт» назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ИС

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			«Сайт», в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по обеспечению безопасности ПДн; – Проводится обучение пользователей ИС «Сайт» мерам по обеспечению безопасности ПДн и предупреждение об ответственности за их несоблюдение; – Не используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Пользователи ИС «Сайт» имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за обеспечение безопасности ПДн; – Программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по обеспечению безопасности персональных данных
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Да	– Обслуживающий персонал и лица, обеспечивающие функционирование ИС «Сайт», не имеют возможности находиться в помещениях, где расположена ИС «Сайт», в отсутствие пользователей ИС «Сайт»; – В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода
2.2	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 действий	Да	– В помещениях, в которых происходит обработка ПДн, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, не оснащены входными дверьми с замками; – Не обеспечивается постоянное закрытие дверей помещений, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, на замок и их открытие только для санкционированного прохода; – Корпуса системных блоков не защищены от вскрытия (не опечатаны/не опломбированы)
3.1	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
3.2	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		Высокая стоимость и сложность подготовки реализации возможности
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	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
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного 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
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	Нет	Не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
4.3	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