УТВЕРЖДАЮ

Директор

_____ М.В. Дворникова

«04» октября 2023 г.

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТА И НФОРМАТИЗАЦИИ

АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"

Государственного областного бюджетного профессионального образовательного учреждения «Липецкий колледж строительства, архитектуры и отраслевых технологий»

Липецк
2023

Оглавление

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 ОИ, 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 ОИ 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, 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 ОИ.

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).

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. Настоящий документ содержит результаты оценки угроз безопасности информации (далее – Оценка угроз).

2.1.2. Оценка угроз проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна на объекте информатизации Государственное областное бюджетное профессиональное образовательное учреждение «Липецкий колледж строительства, архитектуры и отраслевых технологий» АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" (далее –ОИ) (с учетом архитектуры и условий его функционирования) и может привести к нарушению безопасности обрабатываемой на объекте информаизации АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования объекта информатизации Государственное областное бюджетное профессиональное образовательное учреждение «Липецкий колледж строительства, архитектуры и отраслевых технологий» АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" – актуальных угроз безопасности информации.

2.2. Источники разработки

– Оценка угроз проведена на основании анализа данных по объему информации с использованием банка данных угроз безопасности информации ФСТЭК России, а также с учетом требований следующих законодательных актов и нормативно-методических документов:

– 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 РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.;

– Методический документ ФСТЭК России, утвержденный 05 февраля 2021 г. «Методика оценки угроз безопасности информации»;

– Приказ ФСТЭК России 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 «Меры защиты информации в государственных информационных системах» утвержденный ФСТЭК России от 11 февраля 2014 г.;

– Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

– Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 г. № 149/7/2/6-432;

– ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;

– ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем.

Классификация уязвимостей информационных систем;

– ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем.

2.3. Оцениваемые угрозы

2.3.1. Документ содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей, и техногенных источников угроз. При этом в настоящем документе 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

Ответственность за обеспечение защиты информации (безопасности)

№	Ответственный за обеспечение защиты информации	Роль	Основание
1.	А.Д. Буланов	Администратор информационной безопасности	Приказ № 244/1-О от 31.08.2023 г.
2.	Е.А. Шклярук	Ответственный за организацию обработки ПДн	Приказ № 252/1-О от 31.08.2023 г.

2.4. Особенности пересмотра Оценки угроз

2.4.1. Настоящий документ может быть пересмотрен:

– по решению на основе периодически проводимых анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений на объекте информатизации;

– 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 ФИС «ФРДО»;

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

– в случаях выявления инцидентов информационной безопасности на объекте информатизации 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. Настоящий документ разработан в отношении АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении".

3.1.2. Основные характеристики объекта информатизации:

Основания создания (функционирования): Федеральная информационная система «Федеральный реестр сведений о докумен-тах об образовании и (или) о квалификации, документах об обучении» введена в эксплуатацию в соответствии с Постановлением Правительства РФ от 31 мая 2021 г. № 825 «О федеральной информационной системе «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении».

Назначение: Обьект информатизации АРМ подключаемый к Федеральной информационной системе "Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении" предназначен для внесения в Федеральную ин-формационную систему «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении», и предоставления Федеральной службе по надзору в сфере образования и науки сведений о документах об образовании, выдаваемых с 1 января 2021 г. лицам, освоившим образовательные программы основного общего, среднего общего, среднего профессионального образования, а также основные про-граммы профессионального обучения..

3.1.3. ПДн, обрабатываемые в ФИС «Федеральный реестр сведений документов об об-разовании и (или) о квалификации, документах об обучении»:Фамилия; Имя; Отчество; Дата рождения; Пол; Адрес проживания; Реквизиты документа, удостоверяющего личность; Образовательное учреждение; Форма обучения; Профильные предметы; Номер класса; Данные о сдаче экзаменов (Категория участника ЕГЭ, Перечень общеобразовательных предметов, выбранных для сдачи ЕГЭ); Код регистрации; Регион сдачи ЕГЭ.

3.1.4. В соответствии с Актом определения уровня защищенности персональных данных на объекте информатизации АРМ подключаемый к Федеральной информационной системе "Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении" (от 31.08.2023 г.) для ОИ определены характе-ристики, указанные в Таблице 2 и установлен **4-й уровень защищенности ПДн.**

Таблица 2. Характеристика ОИ в соответствии с постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Критерий	Характеристика
Категория обрабатываемых персональных данных	Иные
Субъект персональных данных	Субъекты не являются сотрудниками «Оператора»
Объем обрабатываемых персональных данных	менее 100 000
Тип актуальных угроз	Угрозы 3-го типа
Уровень защищенности ПДн	4-й уровень защищенности ПДн

3.2. Состав и архитектура объекта оценки

3.2.1. Состав АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" определен в таблице 3.

Таблица 3 – Состав ОИ

№ п/п	Характеристика	Значение характеристики
1.	Программноаппаратные средства	АРМ – 1 в составе: Монитор – 1 шт. Системный блок – 1 шт. Клавиатура – 1 шт. Мышь – 1 шт.
2.	Общесистемное программное обеспечение	Операционные системы: Windows 7 Pro
4.	Средства защиты информации	ПО ViPNet Client 4.x (версия 4.5) Сертификат ФСБ России № СФ/124-4062 (действителен до 18.05.2024 г.) Kaspersky Endpoint Security 11 for Windows Сертификат ФСТЭК Росии №4068 (действителен до 22.01.2024 г.) СЗИ от НСД "Secret Net Studio" Сертификат ФСТЭК России № 3745 (действителен до 16.05.2025 г.) ПК "Средство анализа защищенности "Сканер-ВС" Сертификат ФСТЭК России № 2204 (действителен до 13.11.2024 г.)

3.2.2. АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" представляет собой локальную систему (комплекс из автоматизированного рабочего места, территориально размещенного в пределах одного здания) 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.	Выделенная	ПАО Ростелеком	Передача (прием) информации	Тип доступа проводной, протоколы HTTP, TCP/IP, POP3

3.2.2.2. Подключение к информационно-телекоммуникационным сетям Государственное областное бюджетное профессиональное образовательное учреждение «Липецкий колледж строительства, архитектуры и отраслевых технологий» – отсутствует.

3.2.2.3. Подключение к информационно-телекоммуникационным сетям иных организаций – присутствует.

3.2.3. Технологии, используемые в ОИ отражены в таблице 5.

Таблица 5 – Технологии, используемые в ОИ

№ п/п	Технология	Используется / Не используется
1.	Съемные носители информации	Не используются
2.	Технология виртуализации	Не используются
3.	Технология беспроводного доступа	Не используются

№ п/п	Технология	Используется / Не используется
4.	Мобильные технические средства	Не используются
5.	Веб-серверы	Не используются
6.	Технология веб-доступа	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. АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" функционирует на базе инфраструктуры Государственное областное бюджетное профессиональное образовательное учреждение «Липецкий колледж строительства, архитектуры и отраслевых технологий».

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 объект информатизации, и применительно к нарушению безопасности информации, обрабатываемой на объекте информатизации.

4.3. На основе анализа исходных данных об объекте информатизации, 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	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)	У1. Ущерб физическому лицу
НП.2	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	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 ОИ, 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 ОИ 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	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
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)	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.5
	Машинный носитель информации в составе средств вычислительной техники	ВВ.1; 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
	Сетевой трафик	ВВ.1; ВВ.2; ВВ.4
	Системное программное обеспечение	ВВ.2; ВВ.3; ВВ.4; ВВ.5
	Средство вычислительной техники	ВВ.1; ВВ.2; ВВ.3; ВВ.4; ВВ.5
	Средство защиты информации	ВВ.2; ВВ.3; ВВ.4; ВВ.5
	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

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 ОИ, – актуальные нарушители.

6.1.2. Процесс определения актуальных нарушителей включал:

6.1.3. 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	не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации обрабатываемой в ИС
2.	Террористические, экстремистские группировки	Дестабилизация деятельности органов государственной власти, организаций; Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества	не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации обрабатываемой в ИС
3.	Преступные группы (криминальные структуры)	Получение финансовой или иной материальной выгоды	Возможные цели реализации угроз безопасности информации предполагают 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
5.	Конкурирующие организации	Получение финансовой или иной материальной выгоды; Получение конкурентных преимуществ	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды; 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
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды; 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	отсутствует техническая возможность реализации угроз, не используются услуги поставщиков вычислительных услуг, передача информации осуществляется по защищённому каналу связи
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные 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; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
11.	Авторизованные пользователи систем и сетей	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
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

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

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

6.1.3.3. Сопоставление возможных нарушителей и их целей реализации угроз безопасности информации с возможными негативными последствиями и видами рисков (ущерба) от реализации (возникновения) угроз безопасности информации (Приложение № 1). 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 ОИ негативным последствиям и соответствующим рискам (видам ущерба).

6.1.4. Итоговые характеристики возможных нарушителей представлены в таблице 10.

Таблица 10 – Характеристики возможных нарушителей

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
1.	Преступные группы (криминальные структуры)	Внешний	Н4. Нарушитель, обладающий высокими возможностями	Да
2.	Отдельные физические лица (хакеры)	Внешний	Н4. Нарушитель, обладающий высокими возможностями	Да
3.	Конкурирующие организации	Внешний	Н4. Нарушитель, обладающий высокими возможностями	Да
4.	Разработчики программных, программно-аппаратных средств	Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да
5.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н4. Нарушитель, обладающий высокими возможностями	Да
6.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да
7.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да
8.	Авторизованные пользователи систем и сетей	Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да
9.	Системные администраторы и администраторы безопасности	Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да
10.	Бывшие (уволенные) работники (пользователи)	Внешний	Н4. Нарушитель, обладающий высокими возможностями	Да
Предположения о сговоре нарушителей*				
11.	Преступные группы (криминальные структуры) в сговоре с лицами, обеспечивающими функционирование систем и сетей или обеспечивающие системы оператора, авторизованными	Внешний, Внутренний	Н4. Нарушитель, обладающий высокими возможностями	Да

№ п/п	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность
	пользователями систем и сетей, системными администраторами и администраторы безопасности			

6.1.5. 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 ОИ, 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 ОИ. К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам ОИ.

6.1.6. 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.

6.1.7. 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.

6.1.8. 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.

6.1.9. Подробное описание уровней возможностей нарушителей по реализации угроз безопасности информации приведено в Приложении № 2.

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 ОИ, – 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 ОИ;

– о группах пользователей ОИ, 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)
Преступные группы (криминальные структуры)	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
			Механизм обновления BIOS/UEFI	СР.1; СР.2; СР.9
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; 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

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Доступ через средства вычислительной техники	СР.1; СР.8; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; СР.8; СР.9; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.10
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.4; СР.7; СР.9; СР.11
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9; СР.11
			Физический доступ к машинным носителям информации	СР.8; СР.11
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			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; СР.11
			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.4; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
Отдельные физические лица (хакеры)	Внешний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; 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)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
Конкурирующие организации	Внешний	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)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
		Учетные данные пользователя	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
Разработчики программных, программно-аппаратных средств	Внутренний	Сетевое программное обеспечение	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
		Системное программное обеспечение	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
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Средство вычислительной техники	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2
			Физический доступ к программно-аппаратным средствам обработки информации	СР.3; СР.8; СР.9; СР.11
		Средство защиты информации	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Узел вычислительной сети (автоматизированные рабочие места)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.8; СР.11
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
		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
		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
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

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Сетевое оборудование	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; 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.8; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
			Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Узел вычислительной сети (автоматизированные рабочие места)	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; СР.8; СР.9; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.10
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.4; СР.7; СР.9; СР.11
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9; СР.11
			Физический доступ к машинным носителям информации	СР.8; СР.11
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; 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; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			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.4; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; СР.9
Авторизованные пользователи систем и сетей	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.4; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9
		Средство вычислительной техники	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; СР.3; СР.8; СР.9; СР.11
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; СР.9

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			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.8; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; СР.8; СР.9; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.10
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.4; СР.7; СР.9; СР.11
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
			Доступ через средства вычислительной техники	СР.8; СР.9; СР.11

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Машинный носитель информации в составе средств вычислительной техники	Физический доступ к машинным носителям информации	СР.8; СР.11
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; 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; СР.11
			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.4; СР.9; СР.12
			Доступ через средства вычислительной техники	СР.1; СР.3; СР.4; СР.8; 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.4; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.3; СР.4; СР.5; СР.8; СР.9; СР.11
		Сетевой трафик	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10; СР.12

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
		Системное программное обеспечение	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.4; СР.9
			Доступ через средства вычислительной техники	СР.1; СР.2; СР.3; СР.4; СР.8; СР.9
			Пользовательский интерфейс работы с системным программным обеспечением	СР.1; СР.2; 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.8; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам защиты информации	СР.8; СР.11
		Узел вычислительной сети (автоматизированные рабочие места)	Каналы связи узлов локальной вычислительной сети	СР.1; СР.2; СР.9; СР.12
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.2; СР.9; СР.12
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.2; СР.8; СР.9; СР.11
			Графический интерфейс локального взаимодействия пользователя с узлом вычислительной сети	СР.2; СР.9
		Защищаемая информация	Каналы связи узлов локальной вычислительной сети	СР.1; СР.4; СР.9; СР.10

Вид нарушителя	Категория нарушителя	Объекты воздействия	Доступные интерфейсы	Способы реализации (идентификатор)
			Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.4; СР.9; СР.10
			Доступ через средства вычислительной техники	СР.1; СР.4; СР.9; СР.11
			Физический доступ к программно-аппаратным средствам обработки информации	СР.1; СР.4; СР.7; СР.9; СР.11
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; СР.9; СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; СР.9
		Машинный носитель информации в составе средств вычислительной техники	Доступ через средства вычислительной техники	СР.8; СР.9; СР.11
			Физический доступ к машинным носителям информации	СР.8; СР.11
		Учетные данные пользователя	Каналы связи узлов локальной вычислительной сети	СР.1; СР.9; 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
Бывшие (уволенные) работники (пользователи)	Внешний	Сетевое оборудование	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.1; 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
		Файлы cookies	Каналы связи с внешними информационно-телекоммуникационными сетями	СР.10
			Доступ к объектам файловой системы - файлам cookies	СР.1; 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 ОИ – 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 № 3.

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 № 4.

8.3. По результатам оценки возможных угроз безопасности выявлено актуальных угроз: 89. Итоговый перечень актуальных угроз безопасности информации представлен в таблице 13. Выводы об актуальности угроз безопасности информации с приведенными сценариями их реализации представлены в Приложении № 5.

Таблица 13 – Актуальные угрозы безопасности информации

№	Идентификатор угрозы	Наименование угрозы
1.	УБИ.004	Угроза аппаратного сброса пароля BIOS
2.	УБИ.005	Угроза внедрения вредоносного кода в BIOS
3.	УБИ.007	Угроза воздействия на программы с высокими привилегиями
4.	УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации
5.	УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
6.	УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
7.	УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
8.	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
9.	УБИ.018	Угроза загрузки нештатной операционной системы
10.	УБИ.019	Угроза заражения DNS-кеша
11.	УБИ.022	Угроза избыточного выделения оперативной памяти
12.	УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы
13.	УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера
14.	УБИ.025	Угроза изменения системных и глобальных переменных

№	Идентификатор угрозы	Наименование угрозы
15.	УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
16.	УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
17.	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
18.	УБИ.033	Угроза использования слабостей кодирования входных данных
19.	УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
20.	УБИ.036	Угроза исследования механизмов работы программы
21.	УБИ.037	Угроза исследования приложения через отчёты об ошибках
22.	УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
23.	УБИ.053	Угроза невозможности управления правами пользователей BIOS
24.	УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
25.	УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
26.	УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
27.	УБИ.069	Угроза неправомерных действий в каналах связи
28.	УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
29.	УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
30.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
31.	УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
32.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
33.	УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
34.	УБИ.088	Угроза несанкционированного копирования защищаемой информации
35.	УБИ.089	Угроза несанкционированного редактирования реестра
36.	УБИ.090	Угроза несанкционированного создания учётной записи пользователя
37.	УБИ.091	Угроза несанкционированного удаления защищаемой информации
38.	УБИ.093	Угроза несанкционированного управления буфером
39.	УБИ.094	Угроза несанкционированного управления синхронизацией и состоянием
40.	УБИ.095	Угроза несанкционированного управления указателями
41.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
42.	УБИ.099	Угроза обнаружения хостов
43.	УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
44.	УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
45.	УБИ.103	Угроза определения типов объектов защиты
46.	УБИ.104	Угроза определения топологии вычислительной сети
47.	УБИ.109	Угроза перебора всех настроек и параметров приложения
48.	УБИ.111	Угроза передачи данных по скрытым каналам
49.	УБИ.114	Угроза переполнения целочисленных переменных
50.	УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации

№	Идентификатор угрозы	Наименование угрозы
51.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
52.	УБИ.117	Угроза перехвата привилегированного потока
53.	УБИ.118	Угроза перехвата привилегированного процесса
54.	УБИ.122	Угроза повышения привилегий
55.	УБИ.123	Угроза подбора пароля BIOS
56.	УБИ.124	Угроза подделки записей журнала регистрации событий
57.	УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
58.	УБИ.130	Угроза подмены содержимого сетевых ресурсов
59.	УБИ.131	Угроза подмены субъекта сетевого доступа
60.	УБИ.132	Угроза получения предварительной информации об объекте защиты
61.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
62.	УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
63.	УБИ.144	Угроза программного сброса пароля BIOS
64.	УБИ.145	Угроза пропуска проверки целостности программного обеспечения
65.	УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
66.	УБИ.150	Угроза сбоя процесса обновления BIOS
67.	УБИ.152	Угроза удаления аутентификационной информации
68.	УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
69.	УБИ.155	Угроза утраты вычислительных ресурсов
70.	УБИ.156	Угроза утраты носителей информации
71.	УБИ.158	Угроза форматирования носителей информации
72.	УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
73.	УБИ.169	Угроза наличия механизмов разработчика
74.	УБИ.174	Угроза «фарминга»
75.	УБИ.175	Угроза «фишинга»
76.	УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
77.	УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
78.	УБИ.182	Угроза физического устаревания аппаратных компонентов
79.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
80.	УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
81.	УБИ.188	Угроза подмены программного обеспечения
82.	УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
83.	УБИ.192	Угроза использования уязвимых версий программного обеспечения
84.	УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
85.	УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
86.	УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
87.	УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
88.	УБИ.212	Угроза перехвата управления информационной системой
89.	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) ОИ определены обобщенные возможности источников атак:

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	Нет
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	Нет
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 № 6.

9.4. Используемые для защиты информации криптосредства должны обеспечить криптографическую защиту по уровню не ниже КС1.

ПРИЛОЖЕНИЕ № 1

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)	Любопытство или желание самореализации (подтверждение статуса)	–	–	–
		Получение финансовой или иной материальной выгоды	–	–	–
2.	Разработчики программных, программно-аппаратных средств	Получение финансовой или иной материальной выгоды	–	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	–	–	–
3.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды	–	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	–	–	–
4.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора	Получение финансовой или иной материальной выгоды	НП.1	НП.2	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1	–	–

№ 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**
		Месть за ранее совершенные действия	НП.1	НП.2	–
5.	Авторизованные пользователи систем и сетей	Любопытство или желание самореализации (подтверждение статуса)	НП.1	–	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1	–	–
		Месть за ранее совершенные действия	НП.1	–	–
6.	Системные администраторы и администраторы безопасности	Получение финансовой или иной материальной выгоды	–	НП.2	–
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1	–	–
		Месть за ранее совершенные действия	–	НП.2	–
7.	Бывшие (уволенные) работники (пользователи)	Получение финансовой или иной материальной выгоды	НП.1	–	–
		Месть за ранее совершенные действия	НП.1	НП.2	–

ПРИЛОЖЕНИЕ № 2
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

ПРИЛОЖЕНИЕ № 3

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.003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Отсутствуют объекты воздействия
УБИ.006	Угроза внедрения кода или данных	Отсутствуют условия, при которых может быть реализована угроза
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Отсутствуют объекты воздействия
УБИ.011	Угроза деавторизации санкционированного клиента беспроводной сети	Отсутствуют объекты воздействия
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути	Отсутствуют объекты воздействия
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL	Отсутствуют объекты воздействия
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.026	Угроза искажения XML-схемы	Отсутствуют объекты воздействия
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам	Отсутствуют объекты воздействия
УБИ.029	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	Отсутствуют объекты воздействия
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Отсутствуют условия, при которых может быть реализована угроза
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Отсутствуют условия, при которых может быть реализована угроза
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	Отсутствуют условия, при которых может быть реализована угроза
УБИ.040	Угроза конфликта юрисдикций различных стран	Отсутствуют объекты воздействия
УБИ.041	Угроза межсайтового скриптинга	Отсутствуют объекты воздействия
УБИ.042	Угроза межсайтовой подделки запроса	Отсутствуют объекты воздействия
УБИ.043	Угроза нарушения доступности облачного сервера	Отсутствуют объекты воздействия
УБИ.044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Отсутствуют объекты воздействия
УБИ.046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Отсутствуют объекты воздействия
УБИ.047	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	Отсутствуют объекты воздействия
УБИ.048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Отсутствуют объекты воздействия
УБИ.049	Угроза нарушения целостности данных кеша	Отсутствуют объекты воздействия
УБИ.050	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	Отсутствуют объекты воздействия
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	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.059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.060	Угроза неконтролируемого уничтожения информации хранилищем больших данных	Отсутствуют объекты воздействия
УБИ.061	Угроза некорректного задания структуры данных транзакции	Отсутствуют условия, при которых может быть реализована угроза
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	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.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Отсутствуют объекты воздействия
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи	Отсутствуют объекты воздействия
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Отсутствуют объекты воздействия
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Отсутствуют объекты воздействия
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Отсутствуют объекты воздействия
УБИ.079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Отсутствуют объекты воздействия
УБИ.080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	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.084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	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.108	Угроза ошибки обновления гипервизора	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.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Отсутствуют условия, при которых может быть реализована угроза
УБИ.119	Угроза перехвата управления гипервизором	Отсутствуют объекты воздействия
УБИ.120	Угроза перехвата управления средой виртуализации	Отсутствуют объекты воздействия
УБИ.121	Угроза повреждения системного реестра	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	Отсутствуют объекты воздействия
УБИ.128	Угроза подмены доверенного пользователя	Отсутствуют объекты воздействия

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	Отсутствуют условия, при которых может быть реализована угроза
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.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Отсутствуют объекты воздействия
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Отсутствуют условия, при которых может быть реализована угроза
УБИ.159	Угроза «форсированного веб-браузинга»	Отсутствуют объекты воздействия
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Отсутствуют условия, при которых может быть реализована угроза

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.161	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	Отсутствуют объекты воздействия
УБИ.162	Угроза эксплуатации цифровой подписи программного кода	Отсутствуют объекты воздействия
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	Отсутствуют объекты воздействия
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов	Отсутствуют объекты воздействия
УБИ.166	Угроза внедрения системной избыточности	Отсутствуют объекты воздействия
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Отсутствуют объекты воздействия
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Отсутствуют условия, при которых может быть реализована угроза
УБИ.170	Угроза неправомерного шифрования информации	Отсутствуют объекты воздействия
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Отсутствуют объекты воздействия
УБИ.172	Угроза распространения «почтовых червей»	Отсутствуют объекты воздействия
УБИ.173	Угроза «спама» веб-сервера	Отсутствуют объекты воздействия
УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	Отсутствуют условия, при которых может быть реализована угроза
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Отсутствуют объекты воздействия
УБИ.180	Угроза отказа подсистемы обеспечения температурного режима	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
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Отсутствуют объекты воздействия

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
УБИ.189	Угроза маскирования действий вредоносного кода	Отсутствуют условия, при которых может быть реализована угроза
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Отсутствуют объекты воздействия
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Отсутствуют условия, при которых может быть реализована угроза
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	Отсутствуют условия, при которых может быть реализована угроза
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	Отсутствуют условия, при которых может быть реализована угроза
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	Отсутствуют условия, при которых может быть реализована угроза
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.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Отсутствуют условия, при которых может быть реализована угроза

Идентификатор угрозы	Наименование угрозы	Обоснование исключения из числа возможных угроз безопасности информации
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.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Отсутствуют условия, при которых может быть реализована угроза
УБИ.213	Угроза обхода многофакторной аутентификации	Отсутствуют условия, при которых может быть реализована угроза
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Отсутствуют объекты воздействия
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Отсутствуют объекты воздействия
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

ПРИЛОЖЕНИЕ № 4

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
		Т1.12 Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор

№	Тактика	Основные техники
		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
T2	Получение первоначального доступа к компонентам систем и сетей	T2.1 Использование внешних сервисов организации в сетях публичного доступа (Интернет)
		T2.2 Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра
		T2.3 Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке

№	Тактика	Основные техники
		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
		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

№	Тактика	Основные техники
		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
		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

№	Тактика	Основные техники
		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
		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

№	Тактика	Основные техники
		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.
		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

№	Тактика	Основные техники
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, 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

№	Тактика	Основные техники
		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
		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

№	Тактика	Основные техники
		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 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, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов

№	Тактика	Основные техники
		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

ПРИЛОЖЕНИЕ № 5

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.004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.9; СР.11	Сценарий реализации УБИ.004: – Т1 (Т1.9; Т1.15; Т1.16); – Т2 (Т2.9)
УБИ.005	Угроза внедрения вредоносного кода в BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.8	Сценарий реализации УБИ.005: – Т1 (Т1.9; Т1.16; Т1.22); – Т2 (Т2.5); – Т3 (Т3.2; Т3.17); – Т4 (Т4.6)
УБИ.007	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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)
УБИ.008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Учетные данные пользователя	НП.1; НП.2	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 высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.009: – Т1 (Т1.9); – Т3 (Т3.18); – Т4 (Т4.8)

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 высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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 высокими возможностями	BIOS/UEFI	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Сетевой трафик, Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	СР.1; СР.3; СР.9	Сценарий реализации УБИ.014: – Т1 (Т1.5; Т1.16; Т1.19); – Т2 (Т2.5; Т2.6)
УБИ.018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.8	Сценарий реализации УБИ.018: – Т2 (Т2.5); – Т10 (Т10.2)
УБИ.019	Угроза заражения DNS-кеша	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1	Сценарий реализации УБИ.019: – Т8 (Т8.8)
УБИ.022	Угроза избыточного вы-	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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
	деления оперативной памяти					
УБИ.023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.2	СР.1; СР.4	Сценарий реализации УБИ.023: – Т2 (Т2.7); – Т3 (Т3.7); – Т10 (Т10.3)
УБИ.024	Угроза изменения режимов работы аппаратных элементов компьютера	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.11	Сценарий реализации УБИ.024: – Т2 (Т2.10)
УБИ.025	Угроза изменения системных и глобальных переменных	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.3	Сценарий реализации УБИ.025: – Т10 (Т10.2; Т10.4)
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.2; СР.3	Сценарий реализации УБИ.027: – Т3 (Т3.2); – Т8 (Т8.1)

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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Средство защиты информации	НП.1; НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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 протоколов сетевого/локального обмена данными	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Сетевой трафик, Системное программное обеспечение	НП.1; НП.2	СР.1; СР.3	Сценарий реализации УБИ.034: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5); – Т10 (Т10.1)
УБИ.036	Угроза исследования ме-	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.8	Сценарий реализации УБИ.036: – Т2 (Т2.5)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ханизмов работы программы					
УБИ.037	Угроза исследования приложения через отчёты об ошибках	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.037: – Т1 (Т1.9); – Т2 (Т2.5; Т2.6)
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	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.053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.11	Сценарий реализации УБИ.053: – Т2 (Т2.5)
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.063: – Т2 (Т2.5); – Т10 (Т10.11)
УБИ.067	Угроза неправомерного ознакомления с	Внутренний нарушитель, обладающий высокими возможностями	Защищаемая информация	НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.067: – Т1 (Т1.13; Т1.14); – Т10 (Т10.1)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	защищаемой информацией					
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.068: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.3)
УБИ.069	Угроза неправомерных действий в каналах связи	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	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 высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.2; СР.8; СР.9	Сценарий реализации УБИ.072: – Т2 (Т2.5); – Т3 (Т3.8; Т3.18); – Т4 (Т4.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Машинный носитель информации в составе средств вычислительной техники, Учетные данные пользователя	НП.1; НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.074: – Т1 (Т1.12); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Защищаемая информация	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Учетные данные пользователя	НП.2	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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.1; СР.9	Сценарий реализации УБИ.087: – Т1 (Т1.5; Т1.9; Т1.16); – Т2 (Т2.5)
УБИ.088	Угроза несанкционирован-	Внешний нарушитель, обладающий высокими возможностями,	Защищаемая информация, Машин-	НП.1; НП.2	СР.1	Сценарий реализации УБИ.088: – Т2 (Т2.4; Т2.9);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	ного копирования защищаемой информации	Внутренний нарушитель, обладающий высокими возможностями	ный носитель информации в составе средств вычислительной техники			– Т10 (Т10.1)
УБИ.089	Угроза несанкционированного редактирования реестра	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Защищаемая информация, Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.091: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.8)
УБИ.093	Угроза несанкционированного управления буфером	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1	Сценарий реализации УБИ.093: – Т1 (Т1.9); – Т2 (Т2.4; Т2.5); – Т3 (Т3.2); – 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.094	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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 высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1	Сценарий реализации УБИ.098: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3); – Т10 (Т10.1)
УБИ.099	Угроза обнаружения хостов	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.8; СР.9	Сценарий реализации УБИ.100: – Т2 (Т2.4; Т2.5); – Т4 (Т4.1); – Т6 (Т6.6)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.102: – Т2 (Т2.5)
УБИ.103	Угроза определения типов объектов защиты	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.8; СР.9	Сценарий реализации УБИ.103: – Т1 (Т1.1; Т1.3); – Т2 (Т2.4)
УБИ.104	Угроза определения топологии вычислительной сети	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1	Сценарий реализации УБИ.104: – Т1 (Т1.4; Т1.5; Т1.22); – Т2 (Т2.3)
УБИ.109	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.109: – Т2 (Т2.5; Т2.6); – Т10 (Т10.10)
УБИ.111	Угроза передачи данных по скрытым каналам	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Сетевой трафик, Системное программное обеспечение	НП.2	СР.1; СР.8	Сценарий реализации УБИ.111: – Т2 (Т2.4); – Т9 (Т9.10; Т9.12)
УБИ.114	Угроза переполнения целочисленных переменных	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	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 высокими возможностями	Сетевой трафик	НП.2	СР.1; СР.9	Сценарий реализации УБИ.116: – Т1 (Т1.3); – Т2 (Т2.4; Т2.5; Т2.11)
УБИ.117	Угроза перехвата привилегированного потока	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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.122	Угроза повышения привилегий	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.2; СР.8	Сценарий реализации УБИ.122: – Т2 (Т2.5); – Т3 (Т3.5); – Т6 (Т6.1);

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
						– Т10 (Т10.3)
УБИ.123	Угроза подбора пароля BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Средство защиты информации	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.124: – Т1 (Т1.22); – Т2 (Т2.5; Т2.11); – Т7 (Т7.6)
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	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 высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.130: – Т1 (Т1.5); – Т2 (Т2.5; Т2.11); – Т10 (Т10.2)
УБИ.131	Угроза подмены субъекта сетевого доступа	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1	Сценарий реализации УБИ.131: – Т1 (Т1.2); – 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.132	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.132: – Т1 (Т1.5; Т1.6; Т1.17)
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Сетевой трафик, Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9; СР.12	Сценарий реализации УБИ.140: – Т2 (Т2.3; Т2.5); – Т10 (Т10.10)
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	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 высокими возможностями	BIOS/UEFI	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.2	Сценарий реализации УБИ.145: – Т2 (Т2.4; Т2.5; Т2.8); – 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.149	Угроза сбоя обработки специальным образом изменённых файлов	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	СР.1; СР.4	Сценарий реализации УБИ.149: – Т1 (Т1.5); – Т2 (Т2.5); – Т10 (Т10.10)
УБИ.150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	СР.9	Сценарий реализации УБИ.150: – Т1 (Т1.5); – Т2 (Т2.5); – Т4 (Т4.6)
УБИ.152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Учетные данные пользователя	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.152: – Т1 (Т1.22); – Т2 (Т2.4; Т2.11); – Т10 (Т10.10)
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	BIOS/UEFI	НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Сетевой трафик, Системное программное обеспечение, Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	СР.1; СР.8	Сценарий реализации УБИ.155: – Т1 (Т1.5; Т1.9); – Т2 (Т2.3; Т2.5; Т2.11); – 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.156	Угроза утраты носителей информации	Внутренний нарушитель, обладающий высокими возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.156: – Т1 (Т1.10); – Т10 (Т10.1; Т10.8)
УБИ.158	Угроза форматирования носителей информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Машинный носитель информации в составе средств вычислительной техники	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.158: – Т2 (Т2.2; Т2.5); – Т10 (Т10.8)
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	СР.1; СР.9	Сценарий реализации УБИ.163: – Т1 (Т1.3); – Т2 (Т2.5); – Т10 (Т10.1)
УБИ.169	Угроза наличия механизмов разработчика	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.169: – Т2 (Т2.5; Т2.6); – Т3 (Т3.12)
УБИ.174	Угроза «фарминга»	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1; СР.2	Сценарий реализации УБИ.174: – Т1 (Т1.1; Т1.8); – Т3 (Т3.3)
УБИ.175	Угроза «фишинга»	Внешний нарушитель, обладающий высокими возможностями	Сетевой трафик	НП.1; НП.2	СР.1	Сценарий реализации УБИ.175: – Т1 (Т1.1; Т1.11); – Т2 (Т2.8)
УБИ.177	Угроза неподтверждённого ввода данных оператором в	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.177: – Т10 (Т10.14)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
	систему, связанную с безопасностью					
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	СР.1; СР.3	Сценарий реализации УБИ.178: – Т2 (Т2.4; Т2.5); – Т10 (Т10.5)
УБИ.182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель, обладающий высокими возможностями	Средство вычислительной техники	НП.1; НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Средство защиты информации	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.185: – Т2 (Т2.4); – Т7 (Т7.4)
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Средство защиты информации	НП.1; НП.2	СР.1; СР.8; СР.9	Сценарий реализации УБИ.187: – Т2 (Т2.4); – Т7 (Т7.4); – 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.188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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 высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.2; СР.8; СР.9	Сценарий реализации УБИ.191: – Т3 (Т3.2)
УБИ.192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	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	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Средство вычислительной техники	НП.1; НП.2	СР.1; СР.2; СР.8	Сценарий реализации УБИ.203: – Т2 (Т2.5); – Т3 (Т3.2); – Т6 (Т6.3); – Т9 (Т9.11)
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Средство вычислительной техники	НП.1; НП.2	СР.2; СР.8	Сценарий реализации УБИ.208: – Т10 (Т10.11)

Идентификатор угрозы	Наименование угрозы	Характеристика нарушителя, необходимая для реализации угрозы	Объект воздействия	Негативные последствия	Способы реализации угрозы	Возможные сценарии реализации угрозы
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.9	Сценарий реализации УБИ.210: – Т2 (Т2.5); – Т3 (Т3.8); – Т10 (Т10.2; Т10.6)
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.2	СР.1; СР.9	Сценарий реализации УБИ.211: – Т10 (Т10.2)
УБИ.212	Угроза перехвата управления информационной системой	Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение, Средство вычислительной техники	НП.1; НП.2	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.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внешний нарушитель, обладающий высокими возможностями, Внутренний нарушитель, обладающий высокими возможностями	Системное программное обеспечение	НП.1; НП.2	СР.1; СР.2	Сценарий реализации УБИ.217: – Т3 (Т3.8); – Т7 (Т7.24)

ПРИЛОЖЕНИЕ № 6

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	Нет	– Обслуживающий персонал и лица, обеспечивающие функционирование ОИ, не имеют возможности находиться в помещениях, где расположена ОИ, в отсутствие пользователей ОИ; – Работа пользователей ОИ регламентирована; – Ответственный за защиту информации, администраторы ОИ назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ОИ, в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по защите информации; – В помещениях, в которых происходит обработка защищаемой информации, невозможно нахождение посторонних лиц; – Проводится обучение пользователей ОИ мерам по защите информации и предупреждение об ответственности за их несоблюдение; – Используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Ответственный пользователь криптосредств назначается 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	Нет	– Ответственный пользователь криптосредств назначается из числа особо доверенных лиц;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ		– Документация на СКЗИ хранится у ответственного пользователя криптосредств в металлическом сейфе (шкафу); – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками; – 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 ОИ регламентирована; – Проводится обучение пользователей ОИ мерам по защите информации и предупреждение об ответственности за их несоблюдение; – Сведения о физических мерах защиты объектов, в которых размещена ОИ, 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	Нет	– Работа пользователей ОИ регламентирована; – Ответственный за защиту информации, администраторы ОИ назначаются из числа особо доверенных лиц; – Ремонт, обслуживание и сопровождение программных, технических и программно-технических средств ОИ, в том числе СЗИ, выполняется доверенными лицами, с выполнением мер по защите информации; – Проводится обучение пользователей ОИ мерам по защите информации и предупреждение об ответственности за их несоблюдение;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
			– Используются сертифицированные средства защиты информации от НСД; – Используются сертифицированные средства антивирусной защиты, базы вирусных сигнатур регулярно обновляются; – Пользователи ОИ не имеют возможности запуска стороннего или установки, изменения настроек имеющегося программного обеспечения без контроля со стороны ответственного за защиту информации; – Программные, технические, программно-технические средства, в том числе и СЗИ, настроены доверенными лицами и соответствуют требованиям по защите информации
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	Нет	– Обслуживающий персонал и лица, обеспечивающие функционирование ОИ, не имеют возможности находиться в помещениях, где расположена ОИ, в отсутствие пользователей ОИ; – В помещениях, в которых происходит обработка защищаемой информации, невозможно нахождение посторонних лиц; – Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками; – 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	Нет	– В помещениях, в которых происходит обработка защищаемой информации, невозможно нахождение посторонних лиц;

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
	направленными на предотвращение и пресечение несанкционированных действий		– Помещения, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФК, оснащены входными дверьми с замками; – 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 защищены от вскрытия (опечатаны/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

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование
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