УТВЕРЖДАЮ

»

_____
М.П.

«____» _____2024 г.

УТВЕРЖДАЮ

_____
М.П.

«____» _____2024 г.

МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

информационных систем персональных данных

Москва 2024

Содержание

1. Общие положения

1.1. Назначение и область действия документа

В настоящем документе приведена Модель угроз и нарушителя безопасности информации (далее – Модель угроз и нарушителя) информационных систем персональных данных Заказчика (далее - ИСПДн):

– Медицинская информационная система (далее - МИС).

Модель угроз и нарушителя является документом, на основании которого формируются требования к системе защиты персональных данных (исходя из перечня актуальных угроз информации и требований к уровню защищенности) для ИСПДн.

Модель угроз и нарушителя подлежит периодическому пересмотру с целью уточнения:

– области действия – состава типов объектов защиты информационной инфраструктуры ИСПДн;

– факторов (уязвимостей), обуславливающих наличие угроз ИБ;

– потенциальных способов (методов) реализации угроз ИБ;

– видов возможных последствий от реализации угроз ИБ;

– состава источников угроз и нарушителей ИБ;

– потенциала и мотивации нарушителей ИБ.

1.2. Нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз

Модель угроз и нарушителя разработана в соответствии со следующими нормативными документами:

– Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

– Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 05.02.2021);

– Приказ ФСТЭК 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»;

– «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» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432);

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК РФ 14.02.2008)

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности» (утверждены ФСБ России 10 июля 2014 г. N 378).

1.3. Наименование обладателя информации, заказчика, оператора ИСПДн

Обладателем информации, заказчиком и оператором ИСПДн является Заказчик.

Юридический адрес: 127051, г. Москва, Цветной б-р, д. 30, корпус 2

Подразделение, должностные лица, ответственные за обеспечение защиты информации (безопасности) ИСПДн

Подразделением, ответственным за обеспечение безопасности информации в ИСПДн, является Коммерческая федеральная сеть клиник «ООО МЕДИЦИНСКИЕ точноКУЛИКОВА» ОТДЕЛОМ ИБ

2. Описание объекта защиты

2.1. Описание ИСПДн

Перечень ИСПДн и их основные характеристики приведены в таблице (Таблица 1)Таблица 1 – Основные характеристики ИСПДн

	Медицинская информационная система (МИС)
Назначение ИСПДн	Автоматизированная обработка медицинских данных
Архитектура	Клиент - сервер
Местонахождение БД, содержащей ПДн	Москва
Расположение компонентов	В пределах контролируемой зоны
Трансграничная передача ПДн	Нет
Способ обработки ПДн	Автоматизированная с передачей по внутренней сети оператора
Перечень действий с ПДн	Сбор, запись, систематизация, хранение, уточнение (обновление, изменение), использование, передача, распространение, блокирование, удаление и уничтожение.
Категории субъектов ПДн	ПДн субъектов, являющихся пациентами
Категории обрабатываемых ПДн	Иные, специальные
Перечень ПДн	– фамилия, имя и отчество; – данные удостоверения Личности (паспортные данные, военный билет и т.п.); – дата и место рождения; – пол; – полис ОМС; – СНИЛС; – место работы; – сведения об инвалидности; – группа крови; – диагноз
Объем обрабатываемых ПДн	Более 100 000 субъектов
Уровень защищенности ПДн в ИСПДн	УЗ2

2.1. Размещение ИСПДн

Площадки размещения комплекса программно-технических средств ИСПДн представлены в таблице (Таблица 2).

Таблица 2 – Площадки

№ п/п	Адрес площадки	Условное название площадки	Размещаемые ИСПДн
	Москва	Центральный офис	
	Краснодарский край, г. Сочи	Офис 1	МИС
	Ростовская область, г. Ростов-на-Дону	Офис 2	МИС
	Московская область, г. Подольск	Офис 3	МИС
	Свердловская область, г. Екатеринбург	Офис 4	МИС
	Татарстан, г. Казань	Офис 5	МИС
	Ханты-Мансийский автономный округ, г. Ханты-Мансийск	Офис 6	МИС
	Челябинская область, г. Челябинск	Офис 7	МИС
	Самарская область, г. Самара	Офис 8	МИС
	Новосибирская область, г. Новосибирск	Офис 9	МИС
	Волгоградская область, г. Волгоград	Офис 10	МИС
	Калужская область, г. Калуга	Офис 11	МИС
	Алтайский край, г. Барнаул	Офис 12	МИС
	Иркутская область, г. Иркутск	Офис 13	МИС
	Ленинградская область, г. Санкт-Петербург	Офис 14	МИС
	Кировская область, г. Киров	Офис 15	МИС
	Астраханская область, г. Астрахань	Офис 16	МИС

№ п/п	Адрес площадки	Условное название площадки	Размещаемые ИСПДн
	Белгородская область, г. Белгород	Офис 17	МИС
	Ивановская область, г. Иваново	Офис 18	МИС
	Курганская область, г. Курган	Офис 19	МИС
	Тюменская область, г. Тюмень	Офис 20	МИС
	Ямало-Ненецкий автономный округ, г. Салехард	Офис 21	МИС
	Камчатский край, г. Петропавловск-Камчатский	Офис 22	МИС
	Пермский край, г. Пермь	Офис 23	МИС
	Омская область, г. Омск	Офис 24	МИС
	Хабаровский край, г. Хабаровск	Офис 25	МИС
	Тульская область, г. Тула	Офис 26	МИС
	Удмуртская Республика, г. Ижевск	Офис 27	МИС
	Владимирская область, г. Владимир	Офис 28	МИС
	Костромская область, г. Кострома	Офис 29	МИС
	Ставропольский край, г. Ставрополь	Офис 30	МИС

2.2. Структура и состав комплекса программно-технических средств

2.2.1. Серверное оборудование

Серверы ИСПДн и СХД располагаются по адресу: ул. Профсоюзная, д. 123, офис 456, г. Москва.

Перечень серверов и СХД представлен в таблице ниже (Таблица 3).

Таблица 3 – Сервера и СХД

№ п/п	Тип	Имя	Операционная система
	Физический сервер	Server1	Windows Server 2019
	Физический сервер	Server2	CentOS 7
	Физический сервер	Server3	Ubuntu 20.04
	Физический сервер	Server4	Debian 10
	Физический сервер	Server5	Red Hat Enterprise Linux 8
	СХД	Storage1	Linux
	СХД	Storage2	Windows Server 2016
	СХД	Storage3	FreeNAS
	СХД	Storage4	VMware ESXi
	СХД	Storage5	Windows Storage Server 2016

Перечень виртуальных серверов представлен в таблице (Таблица 4).

Таблица 4 – Виртуальные сервера

№ п/п	Тип	Имя	Операционная система	Назначение
	Виртуальный сервер	VM1	Windows Server 2019	МИС
	Виртуальный сервер	VM2	Ubuntu 20.04	МИС
	Виртуальный сервер	VM3	Red Hat Enterprise Linux 8	МИС
	Виртуальный сервер	VM4	CentOS 7	МИС
	Виртуальный сервер	VM5	Windows Server 2019	МИС
	Виртуальный сервер	VM6	CentOS 7	МИС
	Виртуальный сервер	VM7	Debian 10	МИС
	Виртуальный сервер	VM8	Windows Server 2016	МИС
	Виртуальный сервер	VM9	Ubuntu 20.04	МИС

	Виртуальный сервер	VM10	Red Hat Enterprise Linux 8	МИС

2.2.2. Автоматизированные рабочие места

Состав АРМ ИСПДн приведен в таблице (Таблица 5).

Таблица 5 – Автоматизированные рабочие места

№ п/п	ИСПДн	Операционная система	Количество
1	МИС	Windows 10	75

2.3. Сетевая инфраструктура

Коммутация ЛВС Заказчика осуществляется посредством коммутирующего и маршрутизирующего оборудования Aruba (ядро) и Mikrotik.

Перечень активного сетевого оборудования приведен в таблице (Таблица 6)

Таблица 6 – Сетевое оборудование

№ п/п	Тип	Наименование	Модель	Расположение
	Управляемый коммутатор	AM1	Aruba 2930F 48G PoE+ 4SFP+ Switch (JL256A)	Головной офис
	Управляемый коммутатор	AM2	Aruba 3810M 24G 1-slot Switch (JL071A)	Офис 1
	Управляемый коммутатор	AM3	Aruba 2530 24G PoE+ Switch (J9773A)	Офис 2
	Управляемый коммутатор	AM4	Aruba 2930F 24G PoE+ 4SFP Switch (JL261A)	Офис 3
	Управляемый коммутатор	AM5	Aruba 2530 48G PoE+ Switch (J9772A)	Офис 4
	Управляемый коммутатор	AM6	Aruba 2930F 48G PoE+ 4SFP Switch (JL262A)	Офис 5
	Управляемый коммутатор	AM7	Aruba 2540 24G PoE+ 4SFP+ Switch (JL357A)	Офис 6
	Управляемый коммутатор	AM8	Aruba 2930M 24G PoE+ 1-slot Switch (JL320A)	Офис 7
	Управляемый коммутатор	AM9	Aruba 2530 8G PoE+ Switch (J9774A)	Офис 8
	Управляемый коммутатор	AM10	Aruba 2930F 8G PoE+ 2SFP+ Switch (JL258A)	Офис 9

№ п/п	Тип	Наименование	Модель	Расположение
	Маршрутизатор	AM11	Mikrotik CRS326-24G-2S+RM Cloud Router Switch	Головной офис
	Маршрутизатор	AM12	Mikrotik CRS317-1G-16S+RM Cloud Router Switch	Офис 10
	Маршрутизатор	AM13	Mikrotik CRS328-24P-4S+RM Cloud Router Switch	Офис 11
	Маршрутизатор	AM14	Mikrotik CRS312-4C+8XG-RM Cloud Router Switch	Офис 12
	Маршрутизатор	AM15	Mikrotik CRS309-1G-8S+IN Cloud Router Switch	Офис 13
	Маршрутизатор	AM16	Mikrotik CRS112-8P-4S-IN Cloud Router Switch	Офис 14
	Маршрутизатор	AM17	Mikrotik CRS326-24S+2Q+RM Cloud Router Switch	Офис 15
	Маршрутизатор	AM18	Mikrotik CRS354-48G-4S+2Q+RM Cloud Router Switch	Офис 16
	Маршрутизатор	AM19	Mikrotik CRS328-24P-4S+RM Cloud Router Switch	Офис 17
	Маршрутизатор	AM20	Mikrotik CRS309-1G-8S+PC Cloud Router Switch	Офис 18
	Управляемый коммутатор	AM21	Aruba 2930F 48G PoE+ 4SFP Switch (JL260A)	Офис 19
	Управляемый коммутатор	AM22	Aruba 3810M 48G PoE+ 1-slot Switch (JL072A)	Офис 20
	Управляемый коммутатор	AM23	Aruba 2930M 48G PoE+ 1-slot Switch (JL321A)	Офис 21

№ п/п	Тип	Наименование	Модель	Расположение
	Управляемый коммутатор	AM24	Aruba 2540 48G PoE+ 4SFP+ Switch (JL355A)	Офис 22
	Управляемый коммутатор	AM25	Aruba 2930M 48G PoE+ Class4 1-slot Switch (JL322A)	Офис 23
	Маршрутизатор	AM26	Mikrotik CRS326-24S+2Q+RM Cloud Router Switch	Офис 24
	Маршрутизатор	AM27	Mikrotik CRS317-1G-16S+RM Cloud Router Switch	Офис 25
	Маршрутизатор	AM28	Mikrotik CRS328-24P-4S+RM Cloud Router Switch	Офис 26
	Маршрутизатор	AM29	Mikrotik CRS312-4C+8XG-RM Cloud Router Switch	Офис 27
	Маршрутизатор	AM30	Mikrotik CRS309-1G-8S+IN Cloud Router Switch	Офис 28
	Маршрутизатор	AM31	Mikrotik CRS326-24S+2Q+RM Cloud Router Switch	Офис 29
	Маршрутизатор	AM32	Mikrotik CRS326-24S+2Q+RM Cloud Router Switch	Офис 30
	Маршрутизатор	AM33	Mikrotik CRS326-24S+2Q+RM Cloud Router Switch	Офис 14
	Управляемый коммутатор	AM24	Aruba 2930F 48G PoE+ 4SFP Switch (JL260A)	Офис 15

В качестве физической среды передачи информации в ИСПДн используется волоконно-оптический кабель и медный кабель UTP кат. 5E. Для подключения к ИСПДн оконечного оборудования используются установленные в нем сетевые адаптеры с выходными разъемами RJ45. Передача данных в локальной вычислительной сети осуществляется в соответствии со стеками протоколов TCP/IP по технологии Ethernet.

Информационный обмен ПДн между площадками Заказчика производится по защищённым каналам связи.

ЛВС имеет подключение к сетям связи общего пользования с использованием провайдеров:

– Провайдер 1 (500 мбит/с);
– Провайдер 2 (200 мбит/с).

Подключение ЛВС к сетям связи общего пользования осуществляется через МЭ Mikrotik CCR1036-12G-4S.

Беспроводные виды доступа в ИСПДн не используются.

Мобильные технические средства в ИСПДн не используются.

Сетевая схема Заказчика для первых 3 офисов представлена на рисунке 1.

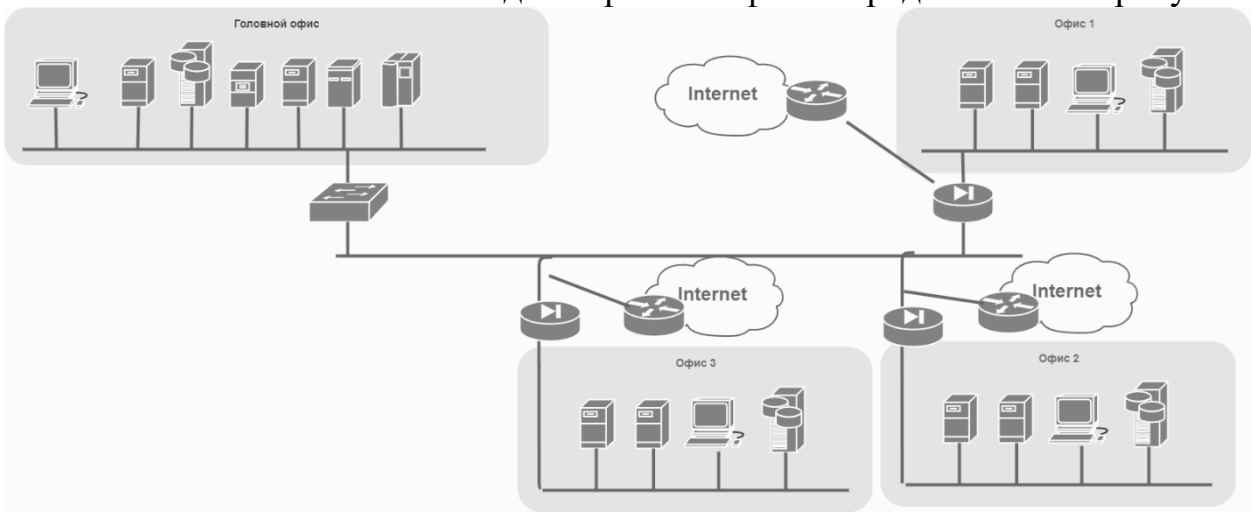

Рисунок 1 - Сетевая схема

2.3.1. Меры и средства технической защиты информации

Сведения о реализации подсистем Системы защиты информации ИСПДн:

Таблица 7 – Реализация подсистем системы защиты информации ИСПДн

№ п/п	Подсистема системы защиты	Описание
	Защита среды виртуализации	Средствами ПО VMware ESXi
	Защита от НСД	Средствами прикладного ПО и AD. Пользователи не имеют прав локального администратора на АРМ. На АРМ не установлены пароли на BIOS.
	Антивирусная защита	Антивирус Касперского 11
	Средство анализа защищенности	Нет
	Межсетевое экранирование	Периметр на границе с Интернет - МЭ Mikrotik
	Защита каналов связи, защита удаленного доступа к ресурсам	Средствами активного сетевого оборудования Mikrotik

№ п/п	Подсистема системы защиты	Описание
	Обнаружение/предотвращение сетевых вторжений	Нет
	Защита от утечек информации	Нет
	Сбор и анализ событий ИБ	Средствами ПО и средств защиты информации
	Резервное копирование	ПО резервного копирования

2.3.2. Организационные меры защиты

Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, осуществляется посредством комплекса организационно-технических мероприятий по физической и технической охране имущественного комплекса Заказчика, включающего в себя:

- круглосуточную физическую охрану имущественного комплекса Заказчика;
- организацию системы пропускного режима на территорию Заказчика;
- использование системы видеонаблюдения и СКУД;
- ограничение доступа в серверные помещения.

Все устройства вывода (отображения) информации ИСПДн (мониторы, принтеры и т.п.) размещены в помещениях Заказчика таким образом, чтобы просмотр информации с экранов, распечаток и т.п. лицами, не допущенными к этой информации, был невозможен. Окна всех помещений Заказчика оборудованы средствами, препятствующими просмотру помещений снаружи (матирование стекол, жалюзи, шторы). В необходимых случаях в помещениях установлены непрозрачные ширмы.

3. Возможные негативные последствия от реализации угроз безопасности информации

Возможные негативные последствия определяются в соответствии с Методикой оценки угроз безопасности информации с учетом оценки вреда, который может быть причинен субъекту, при обработке ПДн в ИСПДн.

Перечень возможных негативных последствий от реализации угроз безопасности информации в ИСПДн приведен в таблице (Таблица 8).

Таблица 8 – Перечень возможных негативных последствий

№	Виды рисков (ущерба)	Возможные негативные последствия
У1	Ущерб физическому лицу	− Нарушение конфиденциальности (утечка) персональных данных
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	− Нарушение законодательства Российской Федерации − 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) − Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)

4. Возможные объекты воздействия угроз безопасности информации

Перечень объектов защиты, воздействия и защищаемой информации ИСПДн формируется путем исключения из базового перечня объектов воздействия, не соответствующих структурно-функциональным характеристикам ИСПДн.

Базовый перечень объектов воздействия представлен следующими объектами (согласно Банку данных угроз безопасности информации ФСТЭК):

- аппаратное обеспечение;
- база данных;
- виртуальная машина;
- виртуальные диски;
- виртуальные устройства;
- виртуальные устройства хранения, обработки и передачи данных;
- виртуальные устройства хранения данных;
- вычислительные узлы суперкомпьютера;
- гипервизор;
- грид-система;
- защищаемые данные;
- информационные ресурсы;
- информационная система;
- информационная система, иммигрированная в облако;
- каналы передачи данных суперкомпьютера;
- каналы связи;
- консоль управления гипервизором;
- консоль управления облачной инфраструктурой;
- машинные носители информации;
- метаданные;
- микропрограммное обеспечение;
- мобильные устройства;
- носители информации;
- облачная инфраструктура;
- облачная инфраструктура, созданная с использованием технологий виртуализации;
- облачная система;
- облачный сервер;
- образ виртуальной машины;
- объекты файловой системы;
- прикладное программное обеспечение;
- программно-аппаратные средства со встроенными функциями защиты;
- рабочая станция;
- реестр;
- ресурсные центры грид-системы;
- сервер;
- сетевое оборудование;
- сетевое программное обеспечение;
- сетевой трафик;

– сетевой узел;
– система разграничения доступа хранилища больших данных;
– система хранения данных суперкомпьютера;
– системное программное обеспечение;
– системное программное обеспечение, использующее реестр;
– средства защиты информации;
– точка беспроводного доступа;
– узлы грид-системы;
– узлы хранилища больших данных;
– учетные данные пользователя;
– хранилище больших данных.

В ИСПДн в качестве объектов защиты рассматриваются следующие основные типы объектов:
– сервер ИСПДн;
– АРМ пользователей и администраторов.

Применимые объекты воздействия угроз безопасности информации к объектам защиты приведены в таблице (Таблица 9).

Таблица 9 – Применимые объекты воздействия угроз безопасности информации

№ п/п	**Тип объекта воздействия**	**Применимость к объектам защиты**	
		сервер ИСПДн	АРМ пользователей и администраторов
	аппаратное обеспечение	Да	Да
	база данных	Да	Нет
	виртуальная машина	Да	Нет
	виртуальные диски	Да	Нет
	виртуальные устройства	Да	Нет
	виртуальные устройства хранения, обработки и передачи данных	Да	Нет
	виртуальные устройства хранения данных	Да	Нет
	вычислительные узлы суперкомпьютера	Нет	Нет
	гипервизор	Да	Нет
	грид-система	Нет	Нет
	защищаемые данные	Да	Нет

№ п/п	Тип объекта воздействия	Применимость к объектам защиты	
		сервер ИСПДн	АРМ пользователей и администраторов
	информационные ресурсы	Да	Нет
	информационная система	Да	Нет
	информационная система, иммигрированная в облако	Нет	Нет
	каналы передачи данных суперкомпьютера	Нет	Нет
	каналы связи	Да	Да
	консоль управления гипервизором	Да	Нет
	консоль управления облачной инфраструктурой	Да	Нет
	машинные носители информации	Да	Нет
	метаданные	Да	Нет
	микропрограммное обеспечение	Да	Да
	мобильные устройства	Нет	Нет
	носители информации	Нет	Нет
	облачная инфраструктура	Нет	Нет
	облачная инфраструктура, созданная с использованием технологий виртуализации	Нет	Нет
	облачная система	Нет	Нет
	облачный сервер	Нет	Нет
	образ виртуальной машины	Нет	Нет
	объекты файловой системы	Нет	Нет
	прикладное программное обеспечение	Да	Да
	программно-аппаратные средства со встроенными функциями защиты	Нет	Нет
	рабочая станция	Да	Да
	реестр	Да	Да
	ресурсные центры грид-системы	Нет	Нет

№ п/п	Тип объекта воздействия	Применимость к объектам защиты	
		сервер ИСПДн	АРМ пользователей и администраторов
	сервер	Да	Нет
	сетевое оборудование	Да	Да
	сетевое программное обеспечение	Да	Да
	сетевой трафик	Да	Да
	сетевой узел	Да	Да
	система разграничения доступа хранилища больших данных	Да	Да
	система хранения данных суперкомпьютера	Нет	Нет
	системное программное обеспечение	Да	Да
	системное программное обеспечение, использующее реестр	Да	Да
	средства защиты информации	Да	Да
	точка беспроводного доступа	Нет	Нет
	узлы грид-системы	Нет	Нет
	узлы хранилища больших данных	Нет	Нет
	учетные данные пользователя	Да	Да
	хранилище больших данных	Нет	Нет

Перечень возможных негативных последствий от реализации угроз безопасности информации и возможные объекты воздействия в ИСПДн приведены в таблице (Таблица 10).

Таблица 10 – Перечень возможных негативных последствий от реализации угроз безопасности информации и возможные объекты воздействия в ИСПДн

№	Негативные последствия	Объекты воздействия	Виды воздействия
П1	Нарушение конфиденциальности (утечка) персональных	1. сервер ИСПДн.	1. Несанкционированный доступ к компонентам, защищаемой информации, системным,

№	Негативные последствия	Объекты воздействия	Виды воздействия
	данных		конфигурационным, иным служебным данным (нарушение конфиденциальности)
П2	Нарушение законодательства Российской Федерации	1. сервер ИСПДн; 2. АРМ пользователей и администраторов.	1. Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным (нарушение конфиденциальности)
П3	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)	1. сервер ИСПДн; 2. АРМ пользователей и администраторов.	1. Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности); 2. Отказ в обслуживании компонентов (нарушение доступности); 3. Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач; 4. Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации/
П4	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации	1. сервер ИСПДн; 2. АРМ пользователей и администраторов.	1. Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности); 2. Отказ в

№	Негативные последствия	Объекты воздействия	Виды воздействия
	функций)		обслуживании компонентов (нарушение доступности); 3. Несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач; 4. Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

5. Источники угроз безопасности информации

5.1. Модель нарушителя

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

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам ИСПДн нарушители подразделяются на две категории:

– внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;

– внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом – мерой усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

– низким потенциалом:

– нарушители с базовыми возможностями по реализации угроз безопасности информации;

– средним потенциалом:

– нарушители с базовыми повышенными возможностями по реализации угроз безопасности информации;

– нарушители со средними возможностями по реализации угроз безопасности информации;

– высоким потенциалом:

– нарушители с высокими возможностями по реализации угроз безопасности информации.

Описание возможных нарушителей приведено в таблице 11.

Таблица 11 – Возможные цели реализации угроз безопасности информации нарушителями

№	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса
2	Террористические, экстремистские группировки	Внешний	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
4	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды

№	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
6	Разработчики программных, программно-аппаратных средств	Внутренний	Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
8	Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ

№	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
13	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия

Оценка целей реализации нарушителями угроз безопасности информации в ИСПДн в зависимости от возможных негативных последствий и видов ущерба от их реализации приведена в таблице (Таблица 12).

Таблица 12 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба

от их реализации

№	Виды нарушителя	Соответствие целей видам ущерба			Оценка актуальности нарушителя
		У1	У2	У3	
	Специальные службы иностранных государств	П1	П2	П3	Актуальный
	Террористические, экстремистские группировки	П2	П2	П3	Актуальный
	Преступные группы (криминальные структуры)	П2	-	-	Актуальный
	Отдельные физические лица (хакеры)	-	-	П1, П2, П3, П4	Актуальный
	Конкурирующие организации	-	-	-	Неактуальный (данный вид нарушителя не достигает своих целей в ИСПДн)
	Разработчики программных, программно-аппаратных средств	П1	П2	П3	Актуальный
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	-	-	Неактуальный (данный вид нарушителя не достигает своих целей в ИСПДн)
	Поставщики вычислительных услуг, услуг связи	-	-	П2	Актуальный
	Лица, привлекаемые для установки,	П1	П4	П1	Актуальный

№	Виды нарушителя	Соответствие целей видам ущерба			Оценка актуальности нарушителя
		У1	У2	У3	
	настройки, испытаний, пусконаладочных и иных видов работ				
	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	-	-	-	Неактуальный (данный вид нарушителя не достигает своих целей в ИСПДн)
	Авторизованные пользователи систем и сетей	-	-	-	Неактуальный (данный вид нарушителя не достигает своих целей в ИСПДн)
	Системные администраторы и администраторы безопасности	-	-	-	Неактуальный (данный вид нарушителя не достигает своих целей в ИСПДн)
	Бывшие работники (пользователи)	П1	П4	-	Актуальный

Таблица 13 – Описание возможностей актуальных нарушителей безопасности информации

Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
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. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	Отдельные физические лица (хакеры) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.). Авторизованные пользователи систем и сетей Бывшие работники (пользователи)

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. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	Преступные группы (криминальные структуры) Конкурирующие организации Поставщики вычислительных услуг, услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы безопасности

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. 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. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в	Террористические, экстремистские группировки Разработчики программных, программно-аппаратных средств

	том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей	

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	Специальные службы иностранных государств

	конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей	

Исходя из таблиц 9 и 13 для ИСПДн характерны следующие типы нарушителей:

- внутренние нарушители с низким потенциалом (Внутренний Н1);
- внешние нарушители с низким потенциалом (Внешний Н1).

Случаи сговора потенциальных внешних нарушителей с внутренними нарушителями не рассматривается по следующим причинам:

- вид нарушителя «Специальные службы иностранных государств» – признан неактуальным для ИСПДн;
- вид нарушителя «Террористические, экстремистские группировки» – признан неактуальным для ИСПДн.

6. Способы реализации угроз безопасности информации

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

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

На основании структурно-функциональных характеристик и особенностей функционирования информационной системы были определены следующие интерфейсы объектов воздействия:

– внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

– внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);

– интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

– интерфейсы для использования съемных машинных носителей информации и периферийного оборудования.

Перечень способов реализации угроз безопасности информации, которые могут быть применены к объектам воздействия ИСПДн, приведен в таблице (Таблица 15).

Таблица 15 – Способы реализации угроз безопасности информации

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
	Бывшие работники (пользователи)	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	внешние сетевые интерфейсы	1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей); –

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
	Поставщики вычислительных услуг, услуг связи	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	1. Сетевые интерфейсы для подключения к локальным и удаленным сетям. 2. Интерфейсы для доступа к базам данных с медицинской информацией. 3. Веб-интерфейсы для удаленного доступа к системе управления данными пациентов. 4. Интерфейсы для обмена данными с другими медицинскими учреждениями или страховыми компаниями. 5. Интерфейсы для обеспечения безопасного доступа к системе извне.	1. Установка и настройка средств защиты информации, таких как антивирусное программное обеспечение, системы обнаружения вторжений, файерволлы и антиспам. 2. Регулярное обновление и патчинг программного обеспечения для закрытия уязвимостей. 3. Реализация механизмов аутентификации и авторизации пользователей для контроля доступа к данным. 4. Шифрование данных при их передаче по сети и хранении на серверах. 5. Организация резервного копирования данных для обеспечения их сохранности и возможности быстрого восстановления после инцидентов. 6. Обучение сотрудников медицинской организации

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				правилам безопасности информации и профилактике утечек данных.
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	сервер ИСПДн	Административные интерфейсы, консоль управления, удаленный доступ по протоколам управления сервером	1. Аутентификация и авторизация: Внедрение механизмов аутентификации пользователей и администраторов, а также установка строгих прав доступа на основе принципа наименьших привилегий. 2. Шифрование данных: Использование шифрования для защиты конфиденциальной информации при передаче данных между сервером и рабочими местами, а также при хранении данных. 3. Мониторинг и аудит: Установка системы мониторинга и аудита для отслеживания действий пользователей, обнаружения аномалий и быстрого реагирования на инциденты
		АРМ пользователей и администраторов	Графический интерфейс пользователя (GUI), командная строка, удаленный доступ к рабочим местам	

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				безопасности. 4. Физическая безопасность: Обеспечение физической безопасности серверов, рабочих мест и другого оборудования, где хранится или обрабатывается конфиденциальная информация. 5. Обучение персонала: Проведение обучения сотрудников по вопросам безопасности информации, правилам работы с ИСПДн и профилактике утечек данных. 6. Регулярное обновление ПО: Внедрение политики регулярного обновления программного обеспечения, патчей и исправлений для минимизации уязвимостей системы. 7. Резервное копирование данных: Создание регулярных резервных копий данных для обеспечения возможности

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				восстановления информации в случае ее утраты или повреждения.
	Разработчики программных, программно-аппаратных средств	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	API, web-интерфейс, консольное управление, удаленный доступ через VPN	1. Внедрение вредоносного кода через уязвимости в программном обеспечении или операционной системе сервера. 2. Манипуляция сетевым трафиком для перехвата данных или осуществления атаки на сервер. 3. Использование слабых паролей или уязвимостей в механизмах аутентификации для несанкционированного доступа. 4. Эксплуатация недостатков в конфигурации сервера для получения привилегированного доступа. 5. Использование социальной инженерии для обмана пользователей или администраторов и получения доступа к серверу. 6. Злоумышленное использование учетных данных уполномоченных

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				пользователей или администраторов для несанкционированного доступа. 7. Внедрение вредоносных программ на сервер для дальнейшего контроля или сбора информации.
	Отдельные физические лица (хакеры)	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	внешние сетевые интерфейсы	1. использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей); − 2. внедрение вредоносного программного обеспечения
	Специальные службы иностранных государств	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	1. Сетевые интерфейсы 2. Веб-интерфейсы 3. Электронная почта	1. Реализация многоуровневой системы защиты 2. Обучение сотрудников 3. Регулярное обновление программного обеспечения 4. Шифрование данных 5. Регулярные аудиты безопасности 6. Управление

№ п/п	Виды нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
				доступом
	Террористические, экстремистские группировки	1. сервер ИСПДн; 2. АРМ пользователей и администраторов	1. Сетевые интерфейсы 2. Пользовательские интерфейсы 3. Удаленные интерфейсы	1. Шифрование данных 2. Многоуровневая аутентификация 3. Установка брандмауэра 4. Мониторинг событий 5. Регулярное обновление ПО
	Преступные группы (криминальные структуры)	сервер ИСПДн	Внешний сетевой интерфейс	1. Реализация комплексной системы защиты информации 2. Обучение персонала правилам безопасности 3. Аудит безопасности и мониторинг системы 4. Разработка и внедрение политик безопасности 5. Регулярное резервное копирование данных
		АРМ пользователей и администраторов	Локальные сетевые интерфейсы	

7. Определение актуальности угроз безопасности информации

7.1. Перечень возможных угроз

По результатам анализа Банка данных угроз ФСТЭК России (далее – БДУ ФСТЭК) выделяются следующие группы угроз (состав групп угроз безопасности информации приведен в Приложении 2):

- угрозы выхода из строя технических средств из-за нарушения физической безопасности и условий эксплуатации;
- угрозы несанкционированного воздействия на BIOS;
- угрозы НСД к системе через компоненты прикладного ПО;
- угрозы НСД к защищаемой информации;
- угрозы несанкционированного воздействия на системные компоненты;
- угрозы НСД к аутентификационной информации;
- угрозы НСД к средствам управления технологическим оборудованием;
- угрозы перехвата управления автоматизированной системой;
- угрозы использования непроверенных компонентов;
- угрозы несвоевременного выявления инцидента ИБ;
- угрозы перехвата информации, передаваемой по каналам связи;
- угрозы подмены участников сетевого взаимодействия;
- угрозы НСД к системе через веб-ресурсы;
- угрозы получения информации о компонентах информационной системы;
- угрозы внедрение вредоносного ПО;
- угрозы «отказа в обслуживании»;
- угрозы НСД к информации, обрабатываемой с использованием технологий виртуализации;
- угрозы НСД к информации, обрабатываемой с использованием технологии грид;
- угрозы НСД к беспроводным каналам передачи данных;
- угрозы НСД к информации, обрабатываемой с использованием облачных услуг;
- угрозы НСД к информации, обрабатываемой с использованием технологии Big Data (хранилище больших данных);
- угрозы НСД к информации, обрабатываемой с использованием суперкомпьютеров;
- угрозы НСД к информации, обрабатываемой с использованием мобильных устройств;
- угрозы НСД к информации, обрабатываемой с использованием технологий машинного обучения.

Оценка применимости перечисленных выше групп угроз к ИСПДн приведена в таблице 16.

Таблица 16 – Оценка применимости групп угроз безопасности

№ п/п	Группы угроз безопасности	Оценка применимости
	Угроза выхода из строя технических средств из-за нарушения физической безопасности и условий эксплуатации	Применима
	Угрозы несанкционированного воздействия на BIOS	Применима
	Угроза НСД к системе через компоненты прикладного ПО	Применима
	Угроза НСД к защищаемой информации	Применима
	Угроза несанкционированного воздействия на системные компоненты	Применима
	Угроза НСД к аутентификационной информации	Применима
	Угроза НСД к средствам управления технологическим оборудованием	Применима
	Угроза перехвата управления автоматизированной системой	Применима
	Угроза использования непроверенных компонентов	Применима
	Угроза несвоевременного выявления инцидента ИБ	Применима
	Угроза перехвата информации, передаваемой по каналам связи	Применима
	Угроза подмены участников сетевого взаимодействия	Применима
	Угроза НСД к системе через веб-ресурсы	Применима
	Угроза получения информации о компонентах информационной системы	Применима
	Угрозы внедрение вредоносного ПО	Применима
	Угроза «отказа в обслуживании»	Применима
	Угроза НСД к информации, обрабатываемой с использованием технологий виртуализации	Применима
	Угроза НСД к информации, обрабатываемой с использованием технологии грид	Не применима (отсутствует объект воздействия)

№ п/п	Группы угроз безопасности	Оценка применимости
	Угрозы НСД к беспроводным каналам передачи данных	Применима
	Угроза НСД к информации, обрабатываемой с использованием облачных услуг	Не применима (отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием технологии Big Data (хранилище больших данных)	Не применима (отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием суперкомпьютеров	Не применима (отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием мобильных устройств	Применима
	Угроза НСД к информации, обрабатываемой с использованием технологий машинного обучения	Применима

Из перечня возможных угроз исключается ряд угроз, для реализации которых требуется потенциал нарушителя выше низкого, поскольку в соответствии с Моделью нарушителя потенциал актуального нарушителя недостаточен для реализации угрозы. Анализ применимости возможных угроз приведен в Приложении 2.

7.2. Сценарии реализации угроз

Для групп угроз безопасности, применимых согласно таблице 16, определяются сценарии реализации. В сценарии реализации угрозы безопасности приводятся следующие сведения:

- источник угрозы (категории нарушителей);
- возможные способы реализации угрозы каждой категорией нарушителей;
- возможные тактики, используемые при реализации угрозы.

Перечень основных техник, соответствующих тактикам реализации угроз безопасности, приведены в Приложении 1.

Сценарии реализации угроз безопасности приведены в таблице 17.

Таблица 17 – Сценарии реализации угроз безопасности

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угроза выхода из строя технических средств из-за нарушения физической безопасности и условий эксплуатации	Внутренний H1	Ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств	T1.1, T1.16	T2.2	T3.5	-	-	-	T7.7	T8.1, T8.8	-	T10.1, T10.8, T10.10
	Угрозы несанкционированного воздействия на BIOS	Внешний H1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угроза НСД к системе через компоненты прикладного ПО	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15
	Угроза НСД к защищаемой информации	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угроза несанкционированного воздействия на системные компоненты	Внешний H1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15
	Угроза НСД к аутентификационной информации	Внешний H1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угроза НСД к средствам управления технологическим оборудованием	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15
	Угроза перехвата управления автоматизированной системой	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				Т1	**Т2**	**Т3**	**Т4**	**Т5**	**Т6**	**Т7**	**Т8**	**Т9**	**Т10**
	Угроза использования непроверенных компонентов	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15
	Угроза несвоевременного выявления инцидента ИБ	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				Т1	**Т2**	**Т3**	**Т4**	**Т5**	**Т6**	**Т7**	**Т8**	**Т9**	**Т10**
	Угроза перехвата информации, передаваемой по каналам связи	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15
	Угроза подмены участников сетевого взаимодействия	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
			системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения										
	Угроза НСД к системе через веб-ресурсы	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угроза получения информации о компонентах информационной системы	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15
	Угрозы внедрение вредоносного ПО	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				Т1	**Т2**	**Т3**	**Т4**	**Т5**	**Т6**	**Т7**	**Т8**	**Т9**	**Т10**
	Угроза «отказа в обслуживании»	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15
	Угроза НСД к информации, обрабатываемой с использованием технологий виртуализации	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
	Угрозы НСД к беспроводным каналам передачи данных	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15
	Угроза НСД к информации, обрабатываемой с использованием мобильных устройств	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	T1.1, T1.9, T1.11	T2.2, T2.3, T2.4, T2.5	T3.4	T4.1, T4.2, T4.3,	-	T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8	T7.1	T8.1, T8.2, T8.3, T8.4, T8.5, T8.6, T8.7	T9.1, T9.2, T93, T9.4, T9.5, T9.6, T9.7, T9.8	T10.15

№ п/п	Угроза безопасности информации	Источник УБИ (нарушитель)	Способы реализации	Тактики и соответствующие им техники, используемые для реализации УБИ									
				Т1	**Т2**	**Т3**	**Т4**	**Т5**	**Т6**	**Т7**	**Т8**	**Т9**	**Т10**
	Угроза НСД к информации, обрабатываемой с использованием технологий машинного обучения	Внешний Н1	1. Использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации системы, а также уязвимостей в процессах обработки данных, может привести к серьезным последствиям 2. Внедрение вредоносного программного обеспечения	Т1.1, Т1.9, Т1.11	Т2.2, Т2.3, Т2.4, Т2.5	Т3.4	Т4.1, Т4.2, Т4.3,	-	Т6.1, Т6.2, Т6.3, Т6.4, Т6.5, Т6.6, Т6.7, Т6.8	Т7.1	Т8.1, Т8.2, Т8.3, Т8.4, Т8.5, Т8.6, Т8.7	Т9.1, Т9.2, Т93, Т9.4, Т9.5, Т9.6, Т9.7, Т9.8	Т10.15

7.3. Актуальные угрозы безопасности информации

По итогам моделирования угроз безопасности информации для ИСПДн определены сценарии реализации угроз безопасности. Согласно данным сценариями актуальными признаны угрозы безопасности информации, приведенные в таблице 18.

Таблица 18 – Актуальные угрозы безопасности информации в ИСПДн

№ п/п	Наименование угрозы	Обозначение угрозы
	Угроза выхода из строя технических средств из-за нарушения физической безопасности и условий эксплуатации	
	Угроза физического устаревания аппаратных компонентов	УБИ.182
	Угроза утраты носителей информации	УБИ.156
	Угрозы несанкционированного воздействия на BIOS	
	Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.009
	Угроза НСД к системе через компоненты прикладного ПО	
	Угроза нарушения целостности данных кеша	УБИ.049
	Угроза пропуска проверки целостности программного обеспечения	УБИ.145
	Угроза использования уязвимых версий программного обеспечения	УБИ.192
	Угроза НСД к защищаемой информации	
	Угроза доступа к защищаемым файлам с использованием обходного пути	УБИ.015
	Угроза использования альтернативных путей доступа к ресурсам	УБИ.028
	Угроза неправомерного ознакомления с защищаемой информацией	УБИ.067
	Угроза несанкционированного восстановления удалённой защищаемой информации	УБИ.071
	Угроза несанкционированного копирования защищаемой информации	УБИ.088
	Угроза форматирования носителей информации	УБИ.158
	Угроза неправомерного шифрования информации	УБИ.170
	Угроза несанкционированной модификации защищаемой информации	УБИ.179

№ п/п	Наименование угрозы	Обозначение угрозы
	Угроза несанкционированного воздействия на системные компоненты	
	Угроза избыточного выделения оперативной памяти	УБИ.022
	Угроза изменения компонентов системы	УБИ.023
	Угроза искажения вводимой и выводимой на периферийные устройства информации	УБИ.027
	Угроза использования механизмов авторизации для повышения привилегий	УБИ.031
	Угроза несанкционированного редактирования реестра	УБИ.089
	Угроза несанкционированного управления буфером	УБИ.093
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	УБИ.115
	Угроза повреждения системного реестра	УБИ.121
	Угроза несанкционированного создания учётной записи пользователя	УБИ.090
	Угроза несанкционированного удаления защищаемой информации	УБИ.091
	Угроза несанкционированного использования системных и сетевых утилит	УБИ.178
	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	УБИ.208
	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	УБИ.209
	Угроза несанкционированного изменения параметров настройки средств защиты информации	УБИ.185
	Угроза НСД к аутентификационной информации	
	Угроза восстановления аутентификационной информации	УБИ.008
	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.030
	Угроза несанкционированного доступа к аутентификационной информации	УБИ.074

№ п/п	Наименование угрозы	Обозначение угрозы
	Угроза несанкционированного изменения аутентификационной информации	УБИ.086
	Угроза обхода некорректно настроенных механизмов аутентификации	УБИ.100
	Угроза удаления аутентификационной информации	УБИ.152
	Угроза использования непроверенных компонентов	
	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем СЗИ	УБИ.205
	Угроза несвоевременного выявления инцидента ИБ	
	Угроза подделки записей журнала регистрации событий	УБИ.124
	Угроза перехвата информации, передаваемой по каналам связи	
	Угроза использования слабостей протоколов сетевого/локального обмена данными	УБИ.034
	Угроза неправомерных действий в каналах связи	УБИ.069
	Угроза перехвата данных, передаваемых по вычислительной сети	УБИ.116
	Угроза подмены участников сетевого взаимодействия	
	Угроза подмены доверенного пользователя	УБИ.128
	Угроза подмены содержимого сетевых ресурсов	УБИ.130
	Угроза получения информации о компонентах информационной системы	
	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	УБИ.098
	Угроза обнаружения хостов	УБИ.099
	Угроза определения типов объектов защиты	УБИ.103
	Угроза определения топологии вычислительной сети	УБИ.104
	Угрозы внедрение вредоносного ПО	
	Угроза внедрения кода или данных	УБИ.006
	Угроза деструктивного изменения конфигурации/среды окружения программ	УБИ.012

№ п/п	Наименование угрозы	Обозначение угрозы
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	УБИ.167
	Угроза скрытного включения вычислительного устройства в состав бот-сети	УБИ.171
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	УБИ.186
	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	УБИ.191
	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	УБИ.217
	Угроза «отказа в обслуживании»	
	Угроза длительного удержания вычислительных ресурсов пользователями	УБИ.014
	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УБИ.113
	Угроза приведения системы в состояние «отказ в обслуживании»	УБИ.140
	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	УБИ.153
	Угроза утраты вычислительных ресурсов	УБИ.155
	Угроза НСД к информации, обрабатываемой с использованием технологий виртуализации	
	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	УБИ.046
	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	УБИ.059
	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	УБИ.078
	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	УБИ.079

№ п/п	Наименование угрозы	Обозначение угрозы
	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	УБИ.084
	Угроза ошибки обновления гипервизора	УБИ.108

7.4. Определение типа актуальных угроз

Согласно Постановлению Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн актуальны угрозы 3-го типа, так как для ИСПДн актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Приложение 1
Перечень основных тактик и техник реализации угроз

№	Тактика	Основные техники	Оценка применимости к ИСПДн
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций	Применима
		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	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		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	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных

№	Тактика	Основные техники	Оценка применимости к ИСПДн
			устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		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	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		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	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем

№	Тактика	Основные техники	Оценка применимости к ИСПДн
			поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем

№	Тактика	Основные техники	Оценка применимости к ИСПДн
			поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера	Неприменима (Виртуализация не применима для сбора информации о подключенных к сети устройствах, их службах и конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений при помощи поисковых систем, пассивного сбора информации о подключенных устройствах, направленного сканирования, сбора информации о пользователях и устройствах путем поиска и эксплуатации уязвимостей, перебора, а также сбора информации, предоставляемой DNS сервисами и при посещении веб-сайтов)
		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	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		T1.10. 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)	Неприменима (Виртуализация не применима для предотвращения кражи цифровых сертификатов и компрометации инфраструктуры доменного регистратора)
		T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга	Применима
		T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами	Неприменима (Виртуализация не применима для предотвращения сбора личной идентификационной информации, доступа к системам физической безопасности, контроля над личными устройствами сотрудников и поиска баз данных на специализированных нелегальных площадках)
		T1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения	Неприменима (Виртуализация не применима для предотвращения сбора личной идентификационной информации, доступа к

№	Тактика	Основные техники	Оценка применимости к ИСПДн
			системам физической безопасности, контроля над личными устройствами сотрудников и поиска баз данных на специализированных нелегальных площадках)
		Т1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации	Неприменима (Виртуализация не применима для предотвращения сбора личной идентификационной информации, доступа к системам физической безопасности, контроля над личными устройствами сотрудников и поиска баз данных на специализированных нелегальных площадках)
		Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках	Неприменима (Виртуализация не применима для предотвращения сбора личной идентификационной информации, доступа к системам физической безопасности, контроля над личными устройствами сотрудников и поиска баз данных на специализированных нелегальных площадках)
		Т1.16. 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	Неприменима (Отсутствуют АСУТП)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		доступа к таким данным через компрометацию подрядчиков и партнеров	
		Т1.17. 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	Неприменима (Отсутствуют АСУТП)
		Т1.18. 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	Неприменима (Отсутствуют АСУТП)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т1.19. 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	Неприменима (Отсутствуют АСУТП)
		Т1.20. 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	Неприменима (Отсутствуют АСУТП)
Т2	Получение первоначального доступа к	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)	Неприменима (Отсутствуют АСУТП)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	компонентам систем и сетей Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий	Т2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра	Применима
		Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке	Применима
		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	Применима
		Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке	Применима
		Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов,	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т2.9. Несанкционированное подключение внешних устройств	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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)	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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)	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т2.13. Реализация атаки типа «человек посередине» для осуществления доступа (например, NTLM/SMB Relaying-атаки)	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации	Неприменима (Не используются системы биометрической аутентификации)
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его программную среду инструментальные средства, необходимые	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	Неприменима (Не используются средства разработки приложений)
		Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей	Неприменима (Не используются средства разработки приложений)
		Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение	Неприменима (Не используются средства разработки приложений)
		Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	ему для дальнейших действий	Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)	Неприменима (Не используются средства разработки приложений)
		Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных	Неприменима (Не используются средства разработки приложений)
		Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе	Неприменима (Не используются средства разработки приложений)
		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	Неприменима (Не используются средства разработки приложений)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Не используются средства разработки приложений)
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах	Неприменима (Не используются средства разработки приложений)
		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	Неприменима (Не используются средства разработки приложений)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Не используются средства разработки приложений)
		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	Неприменима (Не используются средства разработки приложений)
		Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за	Неприменима (Не используются средства разработки приложений)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Не используются средства разработки приложений)
		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	Неприменима (Не используются средства разработки приложений)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
Т4	Закрепление (сохранение доступа) в системе или сети Тактическая задача: получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных	Применима
		Т4.2. Использование штатных средств удаленного доступа и управления операционной системы	Применима
		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	Применима
		Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	управления узлом, изменяет настройки средств защиты и другие действия)	Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
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.	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		Т5.2. Использование штатных средств удаленного доступа и управления операционной системы	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов,

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	Тактическая задача: внедрив вредоносное программное обеспечение или обеспечив постоянное присутствие на узле сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления,		туннелирование трафика и т.д)
		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.)	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		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	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		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	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	который может быть размещен в сети Интернет или в инфраструктуре организации	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	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		Т5.7. Туннелирование трафика управления через VPN	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		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	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		Т5.9. Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов,

№	Тактика	Основные техники	Оценка применимости к ИСПДн
			туннелирование трафика и т.д)
		Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		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.	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
		Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств удаленного управления и обхода средств сетевой фильтрации, таких как использование стандартных и нестандартных портов, туннелирование трафика и т.д)
Т6	Повышение привилегий по доступу к компонентам систем и сетей Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и	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	Применима
		Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи	Применима
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий	Применима
		Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи)	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	получить контроль над узлом	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	Применима
		Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима	Применима
		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	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей.	Применима
		Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды	Неприменима (Виртуализация не применима для предотвращения эксплуатации уязвимостей средств ограничения среды исполнения, таких как виртуальные машины и песочницы, для выполнения кода за пределами этой среды)
Т7	Сокрытие действий и применяемых при этом средств от обнаружения Тактическая задача: нарушитель стремится затруднить применение мер	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения	Применима
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	защиты информации, которые способны помешать его действиям или обнаружить их	Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.13. Создание скрытых файлов, скрытых учетных записей	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки	
		Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.18. Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т7.19. Туннелирование трафика управления через VPN	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
		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	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т7.29. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
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	Применима
		Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям	Применима
		Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	Тактическая задача: получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам	Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям	Применима
		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	Применима
		Т8.6. Копирование вредоносного кода на съемные носители	Применима
		Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей	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	Неприменима (Виртуализация не применима для предотвращения использования 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)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз Тактическая задача: в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы	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	Применима
		Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы	Применима
		Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)	Применима
		Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств	Применима
		Т9.5. Отправка данных по известным протоколам управления и передачи данных	Применима

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия	Т9.6. Отправка данных по собственным протоколам	Применима
		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	Применима
		Т9.8. Туннелирование трафика передачи данных через VPN	Применима
		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	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)
		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	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т9.11. Отправка данных через альтернативную среду передачи данных	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)
		Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)
		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	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)
		Т9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)	Неприменима (Виртуализация ограничивает прямой доступ, что снижает эффективность или делает невозможным выполнение задач)
Т10	Несанкционированный доступ и (или) воздействие на	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках	Неприменима (Отсутствует объект воздействия)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
	информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям Тактическая задача: достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий	Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа	Неприменима (Отсутствует объект воздействия)
		Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения	Неприменима (Отсутствует объект воздействия)
		Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения	Неприменима (Отсутствует объект воздействия)
		Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения	Неприменима (Отсутствует объект воздействия)
		Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства	Неприменима (Отсутствует объект воздействия)
		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	Неприменима (Отсутствует объект воздействия)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей	Неприменима (Отсутствует объект воздействия)
		Т10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)	Неприменима (Отсутствует объект воздействия)
		Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети	Неприменима (Отсутствует объект воздействия)
		Т10.11. Нецелевое использование ресурсов системы.	Неприменима (Отсутствует объект воздействия)
		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	Неприменима (Отсутствует объект воздействия)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Неприменима (Отсутствует объект воздействия)
		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	Неприменима (Отсутствует объект воздействия)

№	Тактика	Основные техники	Оценка применимости к ИСПДн
		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	Применима

Приложение 2
Состав групп угроз безопасности информации

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза выхода из строя технических средств из-за нарушения физической безопасности и условий эксплуатации		
	Угроза преодоления физической защиты	УБИ.139	Применима
	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/ передачи информации	УБИ.157	Применима
	Угроза отказа подсистемы обеспечения температурного режима	УБИ.180	Применима
	Угроза физического устаревания аппаратных компонентов	УБИ.182	Применима
	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	УБИ.160	Применима
	Угроза утраты носителей информации	УБИ.156	Применима
	Угрозы несанкционированного воздействия на BIOS		
	Угроза аппаратного сброса пароля BIOS	УБИ.004	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза внедрения вредоносного кода в BIOS	УБИ.005	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.009	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза деструктивного использования декларированного функционала BIOS	УБИ.013	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза загрузки нештатной операционной системы	УБИ.018	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.024	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования поддельных цифровых подписей BIOS	УБИ.032	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования слабых криптографических алгоритмов BIOS	УБИ.035	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.039	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза нарушения изоляции среды исполнения BIOS	УБИ.045	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза невозможности управления правами пользователей BIOS	УБИ.053	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	УБИ.072	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного использования привилегированных функций BIOS	УБИ.087	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза подбора пароля BIOS	УБИ.123	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза подмены резервной копии программного обеспечения BIOS	УБИ.129	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза программного сброса пароля BIOS	УБИ.144	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза сбоя процесса обновления BIOS	УБИ.150	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза установки уязвимых версий обновления программного обеспечения BIOS	УБИ.154	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза НСД к системе через компоненты прикладного ПО		
	Угроза воздействия на программы с высокими привилегиями	УБИ.007	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования слабостей кодирования входных данных	УБИ.033	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза исследования механизмов работы программы	УБИ.036	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза исследования приложения через отчёты об ошибках	УБИ.037	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза нарушения целостности данных кеша	УБИ.049	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза некорректного задания структуры данных транзакции	УБИ.061	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза некорректного использования функционала программного обеспечения	УБИ.063	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	УБИ.068	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного управления синхронизацией и состоянием	УБИ.094	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного управления указателями	УБИ.095	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза опосредованного управления группой программ через совместно используемые данные	УБИ.102	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перебора всех настроек и параметров приложения	УБИ.109	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза переполнения целочисленных переменных	УБИ.114	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза эксплуатации цифровой подписи программного кода	УБИ.162	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата исключения/сигнала из привилегированного блока функций	УБИ.163	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза подмены действия пользователя путём обмана	УБИ.127	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза пропуска проверки целостности программного обеспечения	УБИ.145	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза наличия механизмов разработчика	УБИ.169	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза подмены программного обеспечения	УБИ.188	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования уязвимых версий программного обеспечения	УБИ.192	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	УБИ.211	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза НСД к защищаемой информации		
	Угроза доступа к защищаемым файлам с использованием обходного пути	УБИ.015	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования альтернативных путей доступа к ресурсам	УБИ.028	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неправомерного ознакомления с защищаемой информацией	УБИ.067	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного восстановления удалённой защищаемой информации	УБИ.071	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного копирования защищаемой информации	УБИ.088	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза форматирования носителей информации	УБИ.158	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза неправомерного шифрования информации	УБИ.170	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированной модификации защищаемой информации	УБИ.179	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза передачи данных по скрытым каналам	УБИ.111	Применима
	Угроза утечки информации с неподключенных к сети Интернет компьютеров	УБИ.203	Применима
	Угроза несанкционированного воздействия на системные компоненты		
	Угроза доступа к локальным файлам сервера при помощи URL	УБИ.016	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза доступа/перехвата/изменения HTTP cookies	УБИ.017	Неприменима (Отсутствует объект воздействия)
	Угроза избыточного выделения оперативной памяти	УБИ.022	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза изменения компонентов системы	УБИ.023	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза изменения системных и глобальных переменных	УБИ.025	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза искажения вводимой и выводимой на периферийные устройства информации	УБИ.027	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования механизмов авторизации для повышения привилегий	УБИ.031	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного редактирования реестра	УБИ.089	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	УБИ.092	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного управления буфером	УБИ.093	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата вводимой и выводимой на периферийные устройства информации	УБИ.115	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата привилегированного потока	УБИ.117	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза перехвата привилегированного процесса	УБИ.118	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза повреждения системного реестра	УБИ.121	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза повышения привилегий	УБИ.122	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	УБИ.143	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного создания учётной записи пользователя	УБИ.090	Применима
	Угроза несанкционированного удаления защищаемой информации	УБИ.091	Применима
	Угроза сбоя обработки специальным образом изменённых файлов	УБИ.149	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного использования системных и сетевых утилит	УБИ.178	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	УБИ.208	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	УБИ.209	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного изменения параметров настройки средств защиты информации	УБИ.185	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного воздействия на средство защиты информации	УБИ.187	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	УБИ.215	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	УБИ.216	Неприменима (Отсутствует объект воздействия)
	Угроза НСД к аутентификационной информации		
	Угроза восстановления аутентификационной информации	УБИ.008	Неприменима (Отсутствует объект воздействия)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию	УБИ.030	Неприменима (Отсутствует объект воздействия)
	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	УБИ.051	Неприменима (Отсутствует объект воздействия)
	Угроза несанкционированного доступа к аутентификационной информации	УБИ.074	Применима
	Угроза несанкционированного изменения аутентификационной информации	УБИ.086	Применима
	Угроза обхода некорректно настроенных механизмов аутентификации	УБИ.100	Применима
	Угроза удаления аутентификационной информации	УБИ.152	Применима
	Угроза «кражи» учётной записи доступа к сетевым сервисам	УБИ.168	Применима
	Угроза перехвата одноразовых паролей в режиме реального времени	УБИ.181	Применима
	Угроза хищения аутентификационной информации из временных файлов cookie	УБИ.197	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	УБИ.201	Применима
	Угроза обхода многофакторной аутентификации	УБИ.213	Применима
	Угроза НСД к средствам управления технологическим оборудованием		
	Угроза отключения контрольных датчиков	УБИ.107	Неприменима (Отсутствует объект воздействия)
	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	УБИ.112	Неприменима (Отсутствует объект воздействия)
	Угроза перехвата управления автоматизированной системой		
	Угроза перехвата управления автоматизированной системой управления технологическими процессами	УБИ.183	Неприменима (Отсутствует объект воздействия)
	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	УБИ.207	Неприменима (Отсутствует объект воздействия)
	Угроза перехвата управления информационной системой	УБИ.212	Неприменима (Отсутствует объект воздействия)
	Угроза использования непроверенных компонентов		

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза включения в проект не достоверно испытанных компонентов	УБИ.165	Применима
	Угроза внедрения системной избыточности	УБИ.166	Применима
	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	УБИ.177	Применима
	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем СЗИ	УБИ.205	Применима
	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	УБИ.210	Применима
	Угроза несвоевременного выявления инцидента ИБ		
	Угроза подделки записей журнала регистрации событий	УБИ.124	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	УБИ.214	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата информации, передаваемой по каналам связи		

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза анализа криптографических алгоритмов и их реализации	УБИ.003	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза использования слабостей протоколов сетевого/локального обмена данными	УБИ.034	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неправомерных действий в каналах связи	УБИ.069	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
4.,	Угроза перехвата данных, передаваемых по вычислительной сети	УБИ.116	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза подмены участников сетевого взаимодействия		
	Угроза заражения DNS-кеша	УБИ.019	Неприменима (Виртуализация не обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя, подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза подмены доверенного пользователя	УБИ.128	Неприменима (Виртуализация не обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя,

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза подмены содержимого сетевых ресурсов	УБИ.130	Неприменима (Виртуализация не обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя, подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза подмены субъекта сетевого доступа	УБИ.131	Неприменима (Виртуализация не обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя, подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза «фарминга»	УБИ.174	Неприменима (Виртуализация не обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя, подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза «фишинга»	УБИ.175	Неприменима (Виртуализация не

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			обеспечивает защиту от угроз, связанных с заражением DNS-кеша, подменой доверенного пользователя, подменой содержимого сетевых ресурсов, подменой субъекта сетевого доступа)
	Угроза НСД к системе через веб-ресурсы		
	Угроза межсайтового скриптинга	УБИ.041	Неприменима (Отсутствует объект воздействия)
	Угроза межсайтовой подделки запроса	УБИ.042	Неприменима (Отсутствует объект воздействия)
	Угроза искажения XML-схемы	УБИ.026	Неприменима (Отсутствует объект воздействия)
	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	УБИ.062	Неприменима (Отсутствует объект воздействия)
	Угроза «форсированного веб-браузинга»	УБИ.159	Неприменима (Отсутствует объект воздействия)
	Угроза «спама» веб-сервера	УБИ.173	Неприменима (Отсутствует объект воздействия)
	Угроза получения информации о компонентах информационной системы		

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	УБИ.098	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза обнаружения хостов	УБИ.099	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза определения типов объектов защиты	УБИ.103	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза определения топологии вычислительной сети	УБИ.104	Применима
	Угроза получения предварительной информации об объекте защиты	УБИ.132	Применима
	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	УБИ.151	Неприменима (Виртуализация обеспечивает защиту веб-сервисов от сканирования благодаря изоляции, управлению доступом и мониторингу)
	Угрозы внедрение вредоносного ПО		
	Угроза внедрения кода или данных	УБИ.006	Неприменима (Виртуализация обеспечивает изоляцию виртуальных машин и контейнеров друг от друга)
	Угроза деструктивного изменения конфигурации/ среды окружения программ	УБИ.012	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза заражения компьютера при посещении неблагонадёжных сайтов	УБИ.167	Применима
	Угроза скрытного включения вычислительного устройства в состав бот-сети	УБИ.171	Применима
	Угроза распространения «почтовых червей»	УБИ.172	Применима
	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	УБИ.186	Применима
	Угроза маскирования действий вредоносного кода	УБИ.189	Применима
	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	УБИ.190	Применима
	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	УБИ.191	Применима
	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	УБИ.193	Применима
	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	УБИ.195	Применима
	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	УБИ.198	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	УБИ.204	Применима
	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	УБИ.217	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза «отказа в обслуживании»		
	Угроза длительного удержания вычислительных ресурсов пользователями	УБИ.014	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УБИ.113	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза приведения системы в состояние «отказ в обслуживании»	УБИ.140	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	УБИ.153	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза утраты вычислительных ресурсов	УБИ.155	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	УБИ.176	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем	УБИ.206	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза НСД к информации, обрабатываемой с использованием технологий виртуализации		
	Угроза выхода процесса за пределы виртуальной машины	УБИ.010	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	УБИ.044	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	УБИ.046	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	УБИ.048	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	УБИ.059	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	УБИ.073	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к виртуальным каналам передачи информации	УБИ.075	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	УБИ.076	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	УБИ.077	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	УБИ.078	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	УБИ.079	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	УБИ.080	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	УБИ.084	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	УБИ.085	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза ошибки обновления гипервизора	УБИ.108	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата управления гипервизором	УБИ.119	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза перехвата управления средой виртуализации	УБИ.120	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза НСД к информации, обрабатываемой с использованием технологии грид		
	Угроза автоматического распространения вредоносного кода в грид-системе	УБИ.001	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза агрегирования данных, передаваемых в грид-системе	УБИ.002	Применима
	Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке	УБИ.047	Применима
	Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы	УБИ.081	Применима
	Угроза перегрузки грид-системы вычислительными заданиями	УБИ.110	Применима
	Угроза распространения несанкционированно повышенных прав на всю грид-систему	УБИ.147	Применима
	Угроза НСД к беспроводным каналам передачи данных		
	Угроза деавторизации санкционированного клиента беспроводной сети	УБИ.011	Применима
	Угроза несанкционированного доступа к системе по беспроводным каналам	УБИ.083	Применима
	Угроза подключения к беспроводной сети в обход процедуры аутентификации	УБИ.125	Применима
	Угроза подмены беспроводного клиента или точки доступа	УБИ.126	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза получения сведений о владельце беспроводного устройства	УБИ.133	Применима
	Угроза НСД к информации, обрабатываемой с использованием облачных услуг		
	Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	УБИ.020	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза злоупотребления доверием потребителей облачных услуг	УБИ.021	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза конфликта юрисдикций различных стран	УБИ.040	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза нарушения доступности облачного сервера	УБИ.043	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения	УБИ.052	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неконтролируемого роста числа виртуальных машин	УБИ.058	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	УБИ.054	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза незащищённого администрирования облачных услуг	УБИ.055	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза некачественного переноса инфраструктуры в облако	УБИ.018	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза некорректной реализации политики лицензирования в облаке	УБИ.064	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неопределённости в распределении ответственности между ролями в облаке	УБИ.065	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза неопределённости ответственности за обеспечение безопасности облака	УБИ.066	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза непрерывной модернизации облачной инфраструктуры	УБИ.070	Неприменима (Потенциал актуального нарушителя недостаточен для их реализации)
	Угроза несогласованности политик безопасности элементов облачной инфраструктуры	УБИ.096	Неприменима (Потенциал актуального нарушителя недостаточен для их

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
			реализации)
	Угроза общедоступности облачной инфраструктуры	УБИ.101	Неприменима (Отсутствует объект воздействия)
	Угроза потери доверия к поставщику облачных услуг	УБИ.134	Неприменима (Отсутствует объект воздействия)
	Угроза потери и утечки данных, обрабатываемых в облаке	УБИ.135	Неприменима (Отсутствует объект воздействия)
	Угроза потери управления облачными ресурсами	УБИ.137	Неприменима (Отсутствует объект воздействия)
	Угроза потери управления собственной инфраструктурой при переносе её в облако	УБИ.138	Неприменима (Отсутствует объект воздействия)
	Угроза приостановки оказания облачных услуг вследствие технических сбоев	УБИ.142	Неприменима (Отсутствует объект воздействия)
	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре	УБИ.164	Неприменима (Отсутствует объект воздействия)
	Угроза привязки к поставщику облачных услуг	УБИ.141	Неприменима (Отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием технологии Big Data (хранилище больших данных)		

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза исчерпания вычислительных ресурсов хранилища больших данных	УБИ.038	Неприменима (Отсутствует объект воздействия)
	Угроза неверного определения формата входных данных, поступающих в хранилище больших данных	УБИ.050	Неприменима (Отсутствует объект воздействия)
	Угроза неконтролируемого копирования данных внутри хранилища больших данных	УБИ.057	Неприменима (Отсутствует объект воздействия)
	Угроза неконтролируемого уничтожения информации хранилищем больших данных	УБИ.060	Неприменима (Отсутствует объект воздействия)
	Угроза несогласованности правил доступа к большим данным	УБИ.097	Неприменима (Отсутствует объект воздействия)
	Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных	УБИ.105	Неприменима (Отсутствует объект воздействия)
	Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных	УБИ.136	Неприменима (Отсутствует объект воздействия)
	Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных	УБИ.148	Неприменима (Отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием суперкомпьютеров		

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами	УБИ.029	Неприменима (Отсутствует объект воздействия)
	Угроза несанкционированного доступа к сегментам вычислительного поля	УБИ.082	Неприменима (Отсутствует объект воздействия)
	Угроза отказа в обслуживании системой хранения данных суперкомпьютера	УБИ.106	Неприменима (Отсутствует объект воздействия)
	Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	УБИ.146	Неприменима (Отсутствует объект воздействия)
	Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	УБИ.161	Неприменима (Отсутствует объект воздействия)
	Угроза НСД к информации, обрабатываемой с использованием мобильных устройств		
	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	УБИ.184	Применима
	Угроза несанкционированного использования привилегированных функций мобильного устройства	УБИ.194	Применима
	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве	УБИ.196	Применима

№ п/п	Наименование угрозы	Обозначение угрозы	Применимость угрозы
	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов	УБИ.199	Применима
	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов	УБИ.200	Применима
	Угроза несанкционированной установки приложений на мобильные устройства	УБИ.202	Применима
	Угроза НСД к информации, обрабатываемой с использованием технологий машинного обучения		
	Угроза раскрытия информации о модели машинного обучения	УБИ.218	Неприменима (Отсутствует объект воздействия)
	Угроза хищения обучающих данных	УБИ.219	Неприменима (Отсутствует объект воздействия)
	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	УБИ.220	Неприменима (Отсутствует объект воздействия)
	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	УБИ.221	Неприменима (Отсутствует объект воздействия)
	Угроза подмены модели машинного обучения	УБИ.222	Неприменима (Отсутствует объект воздействия)

8. Перечень принятых сокращений

8.1. В настоящем документе приняты следующие сокращения:

АРМ	–	Автоматизированное Рабочее Место
ИС	–	Информационная Система
ИСПДн	–	Информационная Система Персональных Данных
ИБ	–	Информационная Безопасность
ЛВС	–	Локальная Вычислительная Сеть
МИС	–	Медицинская Информационная Система
МЭ	–	Межсетевой Экран
НСД	–	Несанкционированный Доступ
ОС	–	Операционная Система
ПК	–	Персональный Компьютер
ПДн	–	Персональные Данные
ПО	–	Программное Обеспечение
СВТ	–	Средства Вычислительной Техники
СЗ	–	Система Защиты Информации
СЗИ	–	Средство Защиты Информации
СЗПДн	–	Система Защиты Персональных Данных
ТС	–	Технические Средства
ФСТЭК России	–	Федеральная Служба По Техническому И Экспортному Контролю Российской Федерации

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ									
ИЗМ.	НОМЕРА ЛИСТОВ (СТРАНИЦ)				ВСЕГО ЛИСТОВ (СТРАНИЦ) В ДОКУМЕНТЕ	НОМЕР ДОКУМЕНТА	ВХОДЯЩИЙ НОМЕР СОПРОВОДИТЕЛЬНОГ О ДОКУМЕНТА И ДАТА	ПОДПИСЬ	ДАТА
	ИЗМЕНЕННЫХ	ЗАМЕНЕННЫХ	НОВЫХ	АННУЛИРОВАН НЫХ					
