Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет прикладной информатики

Дисциплина:

«Основы кибербезопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

«Моделирование угроз безопасности информации в государственной информационной системе»

Выполнил:

Швалов Даниил Андреевич, студент группы К4112с

(подпись)

Проверил:

Кравчук Алексей Владимирович, доцент практики

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

УТВЕРЖДАЮ

_____

(должность)

_____

_____ _____

(подпись) *(инициалы и фамилия)*

«___» _____ 202_ г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ
«Реестр недвижимости Российской Федерации»

Санкт-Петербург
2025

Аннотация

В настоящем документе представлена модель угроз безопасности информации государственной информационной системы «Реестр недвижимости Российской Федерации».

Система представляет собой федеральную информационную систему, в которую вносятся сведения обо всех объектах недвижимости на территории России и их собственниках (далее – Система).

Модель угроз безопасности информации Системы должна являться основой для создания системы защиты информации (далее – СЗИ Системы).

СОДЕРЖАНИЕ

Перечень таблиц

Перечень иллюстраций

Список принятых сокращений и обозначений

Список терминов и определения

ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение и область действия документа

В настоящем документе представлена модель угроз безопасности информации (далее – Модель угроз) при её обработке в Системе. Модель угроз разработана на этапе создания (проектирования) Системы (до ввода объекта в постоянную эксплуатацию) на основе предполагаемых архитектуры и условий функционирования Системы, определенных по результатам изучения и анализа исходных данных о ней.

Модель угроз предназначена для формирования требований по защите информации и обоснования выбора организационно-технических мероприятий и технических средств защиты информации в СЗИ Системы, в том числе, но не ограничиваясь, с учетом архитектуры, технологий, и процесса обработки информации.

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

При разработке Модели угроз использованы банк данных угроз безопасности информации, сформированный ФСТЭК России (bdu.fstec.ru), а также базовые и типовые модели угроз безопасности информации в информационных системах различных классов и типов, согласованных со ФСТЭК России.

Разработка Модели угроз произведена в соответствии с требованиями:

1. Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Постановления Правительства РФ от 06.07.2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».
3. Приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Моделирование угроз осуществлялось в соответствии с подходом, изложенным в «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России 05.02.2021 г. (Информационное сообщение ФСТЭК России от 15 февраля 2021г. №240/22/690) (далее – Методика).

1.3 Обладатель информации (заказчик)

Обладателем информации (заказчиком) Системы является Федеральная служба государственной регистрации, кадастра и картографии.

1.4 Оператор Системы

Оператором Системы является Общество с ограниченной ответственностью «**Роскадастр**» (далее – Общество).

1.5 Структурное подразделение, ответственное за обеспечение безопасности

Ответственным структурным подразделением за обеспечение информационной безопасности в Обществе является Управление информационной безопасности.

2 ОПИСАНИЕ СИСТЕМЫ, ЕЕ ХАРАКТЕРИСТИКА КАК ОБЪЕКТА ЗАЩИТЫ

2.1 Наименование объекта информатизации

2.1.1. Полное наименование: Реестр недвижимости Российской Федерации

2.1.2. Сокращенное наименование: Система.

2.1.3. Решение о создании Системы: Система создается по решению Руководителя Министерства экономического развития Российской Федерации.

2.1.4. Цель создания Системы: Система предназначена для повышения качества и достоверности сведений об объектах недвижимости, развитие и совершенствование предоставления государственных услуг в сфере кадастрового учета и регистрации прав.

2.2 Определение уровня защищенности Системы

По решению Оператора (владельца) в отношении Системы определена необходимость обеспечения 2 класса защищенности, в соответствии с п.14.2 Приказа ФСТЭК России от 11.02.2013 № 17.

2.3 Назначение, задачи (функции) Системы

Система предназначена для хранения всех актуальных сведений о разных объектах недвижимости.

2.4 Системы внешнего информационного взаимодействия Системы

Взаимодействие с внешними информационными системами, а также информационно-телекоммуникационными системами не предполагается.

2.5 Состав информации, планируемой к обработке в Системе

Общество в ходе своей деятельности планирует к обработке в Системе следующие категории защищаемой информации:

- персональные данные;
- конфиденциальные сведения, защищаемые законодательством;
- защищаемая технологическая, конфигурационная, служебная информация;
- общедоступная информация, доступ к которой не ограничивается Федеральными законами Российской Федерации, но может быть ограничен обладателем (оператором) такой информации.

2.5.1. Персональные данные

К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных):

- сведения, идентифицирующие гражданина (ФИО, дата и место рождения, паспортные данные, СНИЛС, ИНН и пр.);
- специальные категории персональных данных (состояние здоровья, национальность, биометрические данные и др.);

– служебные персональные данные сотрудников органов власти (должность, служебные контакты и пр.).

2.5.2. **Информация ограниченного доступа, не относящаяся к персональным данным, а также не содержащая сведения, составляющие государственную тайну**

К сведениям ограниченного доступа относится любая другая информация, подлежащая защите в соответствии с требованиями законодательства РФ или по самостоятельному решению Обладателя информации.

2.5.3. **Общедоступная информация**

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен законодательством РФ, а также Обладателем такой информации.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

2.6 Структура и архитектура Системы

Система имеет клиент-серверную архитектуру, предоставление доступа к ресурсам Системы осуществляется с использованием технологии веб-интерфейса по протоколу HTTP/HTTPS.

Система является федеральной информационной системой. На момент оценки угроз безопасности информации Система планировалась к размещению на базе 30 виртуальных машин, расположенных в составе информационно-телекоммуникационной инфраструктуры центра обработки данных АО «Ростелеком», по адресу: Российская Федерация, г. Москва, 2».

Система имеет прямое подключение к сетям международного информационного обмена, в т.ч. сети «Интернет» по принципу «запрещено всё, что не разрешено».

В качестве базового протокола сетевого взаимодействия используется стек протоколов TCP/IP.

Функционирование Системы предполагается на базе операционной системы Astra Linux Server.

Функционирование СУБД Postgres Pro предполагается на базе операционной системы Astra Linux Server.

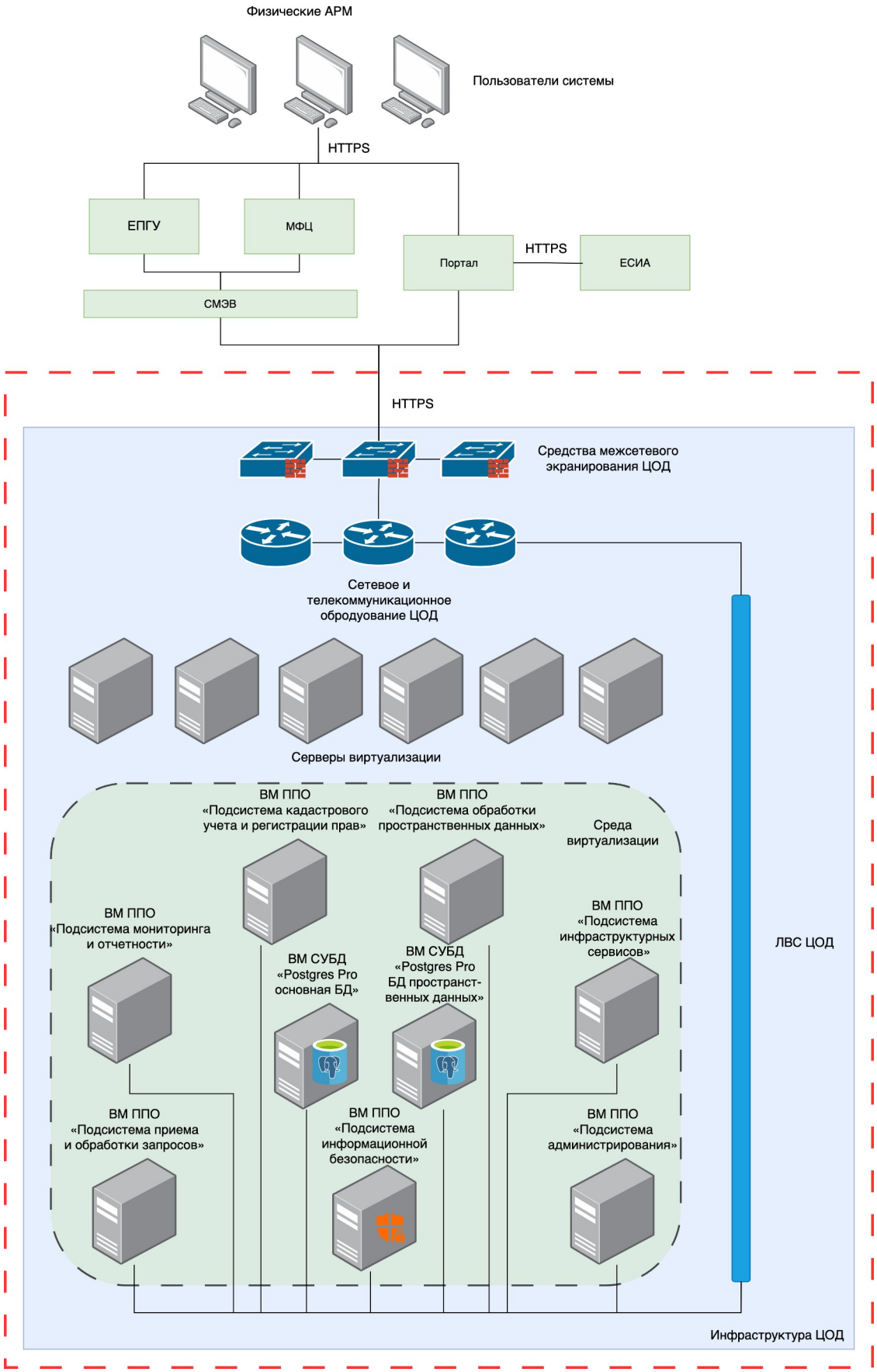

Рисунок **1**. Структурная схема Системы

2.7 Сведения о центре обработки данных, на базе которого размещены ресурсы объекта информатизации

Система планируется к размещению на базе облачной информационно-телекоммуникационной инфраструктуры центра обработки данных АО «Ростелеком» (Облако ИИИ). Облачная инфраструктура имеет следующие подтверждения соответствия требованиям безопасности информации:

- **Аттестат соответствия требованиям о защите информации № 000000.2033 (уч.№ 0000) от «30» декабря 2331** года …;
- **…** .

2.8 Режимы функционирования

Режим функционирования Системы – круглосуточно, исключая согласованные периоды времени на выполнение регламентных работ по обслуживанию оборудования или обновление программного обеспечения Системы. Планируется, что технические работы будут выполняться в часы минимальной пользовательской активности.

2.9 Описание групп внешних и внутренних пользователей Системы

Внутренние непривилегированные и привилегированные пользователи, администрирующие Систему и СЗИ Системы, – это работники организации, которые будут назначены приказами (распоряжениями) по Организации.

2.10 Объекты защиты

Под объектами защиты Системы следует понимать ключевые информационные ресурсы, информационные активы, в том числе активное сетевое оборудование (АСО), серверное оборудование и сервисы (службы), общесистемное программное обеспечение (ОПО), прикладное программное обеспечение (ППО), средства защиты информации, в том числе средства криптографической защиты информации (СЗИ и СКЗИ), обеспечивающие функционирование Системы, воздействие на которые может привести к различным негативным последствиям, в том числе прекращению функционирования Системы в целом или на отдельных участках (линиях связи), или создать предпосылки к реализации угроз безопасности информации (усилить оснащенность источников угроз).

Для обеспечения свойств безопасности информации (конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности ПДн и (или) средств их обработки), и с учетом используемых в Системе информационных технологий, технических средств и программного обеспечения, к объектам защиты относятся:

- информация, обрабатываемая в Системе: персональные данные, конфиденциальные сведения, защищаемые законодательством, коммерческая тайна и информация, признанная конфиденциальной на основании гражданско-правовых Договоров, технологическая, конфигурационная, служебная и иная информация ограниченного доступа, а также общедоступная информация, доступ к которой не ограничивается Федеральными законами Российской Федерации, но может быть ограничен обладателем (оператором) такой информации;

- общесистемное, прикладное, прикладное программное обеспечение Системы;
- системы управления базами данных, размещаемые на базе ВМ (СУБД);
- система (механизмы) резервного копирования для данных СУБД на базе ВМ;
- средства защиты информации (далее – СЗИ), применяемые для защиты информации, в том числе СКЗИ;
- используемые Системой каналы связи (линии связи, сетевой трафик на всех уровнях сети);
- технические средства Системы (в том числе СВТ, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической информации), используемые для обработки информации;
- среды виртуализации (гипервизор, виртуальные машины, образы виртуальных машин, и пр.).
- микропрограммное обеспечение (BIOS / UEFI);
- обеспечивающие подсистемы (температурного режима, электропитания);
- помещения, в которых размещены программно-аппаратные комплексы Системы, а также обеспечивающие подсистемы.

3 ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Перечень потенциальных негативных последствий от реализации (возникновения) угроз безопасности информации разработан на основании экспертной оценки и основывается на базовом перечне негативных последствий, приведенном в Методике с учетом структурно-функциональных характеристик, указанных в Разделе 2 настоящего документа.

Виды рисков (ущербов), актуальных для Оператора, которые могут наступить от нарушения или прекращения основных процессов, а также описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации, может привести к возникновению рисков (ущербов), приведены в таблице ниже (Таблица 1).

Таблица 1. Виды рисков (ущерба) и негативные последствия от реализации угроз безопасности информации

№ п/п	Виды риска (ущерба)	Идентификатор [1]	Возможные негативные последствия
1	2	3	4
1.	У1 Ущерб физическому лицу	У1.1.	Нарушение конфиденциальности (утечка) персональных данных
2.	У2 Ущерб Оператору Системы	У2.1.	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности
		У2.2.	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций
		У2.3.	Простой информационной системы
		У2.4.	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)
		У2.5.	Неспособность выполнения договорных обязательств
		У2.6.	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)
		У2.7.	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)
		У2.8.	Утрата доверия к Обществу
		У2.9.	Недополучение ожидаемой (прогнозируемой) прибыли
		У2.10.	Срыв запланированной сделки с партнером
		У2.11.	Потеря клиентов, поставщиков
		У2.12.	Потеря конкурентного преимущества
		У2.13.	Невозможность заключения договоров, соглашений
		У2.14.	Нарушение деловой репутации
		У2.15.	Снижение престижа
		У2.16	Причинение имущественного ущерба

[1] Идентификатор возможного негативного последствия.

4 ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Целью определения возможных объектов воздействия угроз безопасности информации является выявление информационных ресурсов и компонентов Системы, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям, приведенным в Разделе 3 настоящего документа. Перечень возможных объектов воздействия угроз безопасности информации направлен на определение границ процесса оценки угроз безопасности циркулирующей информации.

Перечень возможных объектов воздействия разработан на основе предполагаемых архитектуры и условий функционирования Системы, определенных по результатам изучения и анализа исходных данных.

Проведение атак на иные объекты защиты, из состава, приведенного в Разделе 2.10 не могут причинить значительный ущерб физическим лицам, Оператору Системы.

В таблице ниже (Таблица 2) приведено описание видов воздействия на компоненты Системы, представляющие собой объекты воздействия, реализация атак на которые может привести к негативным последствиям, приведенным в Разделе 3 настоящего документа.

Таблица 2. Возможные виды воздействия на объекты воздействия

№ п/п	Объекты воздействия	Виды воздействия
1	2	3
1.	**– Нарушение конфиденциальности (утечка) персональных данных (У1.1.); – Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.) (У2.7.).**	
1.1.	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
1.2.	Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
		Несанкционированный доступ к информации, в т.ч. ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)
1.3.	Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
1.4.	Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации, в т.ч. ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)
1.5.	Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации, в т.ч. ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)
1.6.	Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
1.7.	Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)
2.	**– Простой информационной системы (У2.3.); – Неспособность выполнения договорных обязательств (У2.5.); – Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций) (У2.6.); – Недополучение ожидаемой (прогнозируемой) прибыли (У2.9.); – Срыв запланированной сделки с партнером (У2.10.); – Потеря клиентов, поставщиков (У2.11.); – Потеря конкурентного преимущества (У2.12.); – Невозможность заключения договоров, соглашений (У2.13.).**	
2.1.	Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.2.	Прикладное программное обеспечение	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)

№ п/п	Объекты воздействия	Виды воздействия
1	2	3
2.3.	Система управления базой данных (СУБД)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.4.	Системное программное обеспечение (ВМ)	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
		Отказ в обслуживании компонентов (нарушение доступности)
2.5.	Виртуальные машины (образы виртуальной машины)	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.6.	Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
		Отказ в обслуживании компонентов (нарушение доступности)
2.7.	Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.8.	Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.9.	Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.10.	Несъемные носители информации	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
2.11.	Каналы связи (сетевой трафик)	Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)
		Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
		Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)
3.	**– Необходимость дополнительных (незапланированных) затрат на восстановление деятельности (У2.1.);** **– Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств) (У2.4.).**	
3.1.	Прикладное программное обеспечение	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации

№ п/п	Объекты воздействия	Виды воздействия
1	2	3
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.2.	Система управления базой данных (СУБД)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.3.	Виртуальные машины (образы виртуальной машины)	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.4.	Системное программное обеспечение (ВМ)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.5.	Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.6.	Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.7.	Несъемные носители информации	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.8.	Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
3.9.	Аппаратное обеспечение (сетевое оборудование)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
4.	**– Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций (У2.2.); – Утрата доверия к Обществу (У2.8.); – Нарушение деловой репутации (У2.14.); – Снижение престижа (У2.15.); – Причинение имущественного ущерба (У2.16.).**	
4.1.	Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
4.2.	Защищаемые информационные ресурсы ограниченного доступа	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
		Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)
		Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы
4.3.	Прикладное программное обеспечение	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
4.4.	Виртуальные машины (образы виртуальных машин)	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)

№ п/п	Объекты воздействия	Виды воздействия
1	2	3
		Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)
4.5.	Системное программное обеспечение (ВМ)	Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
4.6.	Микропрограммное обеспечение (BIOS / UEFI)	Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
4.7.	Среда виртуализации (Гипервизор)	Отказ в обслуживании компонентов (нарушение доступности)
		Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)
4.8.	Несъемные носители информации	Утечка защищаемой информации, путем НСД к носителям информации
4.9.	Аппаратное обеспечение (сетевое оборудование)	Отказ в обслуживании компонентов (нарушение доступности)
4.10.	Каналы связи (сетевой трафик)	Отказ в обслуживании компонентов (нарушение доступности)

5 ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Определение источников угроз безопасности информации производится с целью последующего определения необходимых мер и средств по предотвращению реализации угроз информационной безопасности Системы.

Определение источников угроз безопасности информации базируется на определении возможных антропогенных источников угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты Системы, – актуальные нарушители.

Определение возможных антропогенных источников угроз безопасности информации содержит предположения о возможностях нарушителя, которые могут быть им использованы для разработки и проведения атак, а также об ограничениях на эти возможности.

5.1. Описание потенциального нарушителя информационной безопасности Системы

Под нарушителем информационной безопасности понимается физическое лицо или организация, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности информации при её обработке в Системе.

Всех нарушителей ИБ целесообразно разделить на две категории:

- **внешних (категория I)** – лица, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
- **внутренних (категория II)** – лица, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Констатируется, что:

- внешними нарушителями могут быть как лица категории I, так и лица категории II;
- внутренними нарушителями могут быть только лица категории II.

Все потенциальные нарушители, вне зависимости от категории, могут обладать следующими видами возможностей:

- базовыми возможностями по реализации угроз безопасности информации (H1);
- базовыми повышенными возможностями по реализации угроз безопасности информации (H2);
- средними возможностями по реализации угроз безопасности информации (H3);
- высокими возможностями по реализации угроз безопасности информации (H4).

Для одной Системы актуальными могут являться нарушители, имеющие разные уровни возможностей.

Отмечается, что внешние нарушители реализуют угрозы безопасности информации **преднамеренно** (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых.

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

В соответствии с БДУ ФСТЭК России (bdu.fstec.ru) различают нарушителей информационной безопасности с высоким, средним и низким потенциалом:

- **высокий потенциал** подразумевает наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей;
- **средний потенциал** подразумевает наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей;
- **низкий потенциал** подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Таблица 3. Виды потенциальных нарушителей безопасности информации Системы

№ п/п	Уровень возможностей нарушителей	Виды нарушителей	Возможные цели реализации угроз безопасности информации	Категория нарушителя	Предположения о потенциале
1	2	3	4	5	6
H1	Нарушитель, обладающий базовыми возможностями	Бывшие работники оператора	● Получение финансовой или иной материальной выгоды; ● Моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; ● Любопытство или желание самореализации (подтверждение статуса); ● Месть за ранее совершенные действия.	Внешний	Низкий
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	● Получение финансовой или иной материальной выгоды. ● Непреднамеренные, неосторожные или неквалифицированные действия. ● Получение конкурентных преимуществ.	Внешний	Низкий
		Отдельные физические лица (хакеры)	● Получение финансовой или иной материальной выгоды. ● Любопытство или желание самореализации (подтверждение статуса)	Внешний	Низкий
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	● Получение финансовой или иной материальной выгоды. ● Непреднамеренные, неосторожные или неквалифицированные действия.	Внутренний	Низкий
		Авторизованные внутренние пользователи Системы	● Получение финансовой или иной материальной выгоды; ● Моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; ● Любопытство или желание самореализации (подтверждение статуса); ● Месть за ранее совершенные действия; ● Непреднамеренные, неосторожные или неквалифицированные действия.	Внешний	Низкий
		Возможности нарушителей по реализации угроз безопасности информации:			
		● 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.**		
H2	Нарушитель, обладающий базовыми повышенными	Преступные группы, - криминальные структуры, хакерские группы	● Получение финансовой или иной материальной выгоды. ● Желание самореализации (подтверждение статуса)	Внешний	Средний
		Лица, привлекаемые для установки, настройки, испытаний,	● Получение финансовой или иной материальной выгоды; ● Непреднамеренные, неосторожные или неквалифицированные	Внутренний	Средний

№ п/п	Уровень возможностей нарушителей	Виды нарушителей	Возможные цели реализации угроз безопасности информации	Категория нарушителя	Предположения о потенциале
1	2	3	4	5	6
	возможностями	пусконаладочных и иных видов работ	действия; ● Получение конкурентных преимуществ.		
		Конкурирующие организации	● Получение конкурентных преимуществ; ● Получение финансовой или иной материальной выгоды	Внешний	Средний
		Поставщики вычислительных услуг, услуг связи	● Получение финансовой или иной материальной выгоды. ● Непреднамеренные, неосторожные или неквалифицированные действия. ● Получение конкурентных преимуществ	Внутренний	Средний
		Администраторы программно-аппаратного комплекса Системы	● Получение финансовой или иной материальной выгоды; ● Любопытство или желание самореализации (подтверждение статуса); ● Месть за ранее совершенные действия; ● Непреднамеренные, неосторожные или неквалифицированные действия.	Внутренний	Средний
		Администраторы системы защиты информации Системы	● Получение финансовой или иной материальной выгоды; ● Любопытство или желание самореализации (подтверждение статуса); ● Месть за ранее совершенные действия; ● Непреднамеренные, неосторожные или неквалифицированные действия.	Внутренний	Средний
		Возможности нарушителей по реализации угроз безопасности информации:			
		● 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.**		
Н3	Нарушитель, обладающий средними возможностями	Террористические, экстремистские группировки	● Совершение террористических актов, угроза жизни граждан. ● Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. ● Дестабилизация общества. ● Дестабилизация деятельности органов государственной власти, организаций	Внешний	Средний
		Разработчики программных, программно-аппаратных средств	● Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки.	Внутренний	Средний

№ п/п	Уровень возможностей нарушителей	Виды нарушителей	Возможные цели реализации угроз безопасности информации	Категория нарушителя	Предположения о потенциале
1	2	3	4	5	6
			● Получение конкурентных преимуществ. ● Получение финансовой или иной материальной выгоды. ● Непреднамеренные, неосторожные или неквалифицированные действия		
		Возможности нарушителей по реализации угроз безопасности информации:			
		● 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 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.**		
Н4	Нарушитель, обладающий высокими возможностями	Специальные службы иностранных государств или блоков государств, в т. ч. иностранные технические разведки	● 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	Внешний	Высокий
		Возможности нарушителей по реализации угроз безопасности информации:			
		● 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.		

№ п/п	Уровень возможностей нарушителей	Виды нарушителей	Возможные цели реализации угроз безопасности информации	Категория нарушителя	Предположения о потенциале
1	2	3	4	5	6
		● Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. ● Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. **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.**		

После определения актуальных источников проводится анализ возможных схем сговора между источниками. Сговор между источниками приводит к повышению их уровня возможностей (потенциала). В таблице ниже представлены типовые схемы сговора. В случае сговора нарушителей цели и уровни возможностей нарушителей подлежат объединению. При этом итоговый потенциал не может быть ниже потенциала, который имеет участник сговора с наивысшим потенциалом.

Таблица 4. Совокупный потенциал нарушителей в случае, если для объекта информатизации сговор нарушителей признается актуальным.

№ п/п	Внешний нарушитель Внутренний нарушитель	Бывшие работники оператора	Лица, обеспечивающие поставку программных, программно-аппаратных средств.	Отдельные физические лица (хакеры)	Преступные группы, - криминальные структуры, хакерские группы	Конкурирующие организации	Террористические, экстремистские группировки	Специальные службы иностранных государств или блоков государств, в т. ч. иностранные технические разведки
1	2	3	4	5	6	7	8	9
1.	**Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)**	Потенциал: низкий, уровень возможностей: Н1	Потенциал: низкий, уровень возможностей: Н1	Потенциал: низкий, уровень возможностей: Н1	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4
2.	**Авторизованные внутренние пользователи Системы**	Потенциал: низкий, уровень возможностей: Н1	Потенциал: низкий, уровень возможностей: Н1	Потенциал: низкий, уровень возможностей: Н1	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4
3.	**Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ**	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4
4.	**Администраторы программно-аппаратного комплекса Системы**	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4
5.	**Администраторы системы защиты информации Системы**	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4
6.	**Поставщики вычислительных услуг, услуг связи**	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н2	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н4
7.	**Разработчики программных, программно-аппаратных средств**	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н3	Потенциал: средний, уровень возможностей: Н3	Потенциал: высокий, уровень возможностей: Н4

5.2. Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Актуальные источники УБИ определяются исходя из особенностей функционирования и организационной структуры Оператора, структурно-функциональных характеристик Системы, критериев определения актуальности источников УБИ и возможных целей реализации УБИ (причин деструктивных воздействий).

В таблице ниже представлены сведения о возможностях (потенциале) источников УБИ.

Таблица 5. Критерии определения актуальных источников УБИ.

№ п/п	Источник угроз	Критерии	Комментарий
1	2	3	4
1.	Специальные службы иностранных государств	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, в следующих случаях: – В Системе обрабатываются сведения, отнесенные к государственной тайне: сведения в военной области, экономики, науки и техники, сведения в области внешней политики и экономики; сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты. – Организация является лидером, занимая значительный объем отраслевого рынка.	Источник неактуален для Оператора, т.к.: – В Системе не обрабатываются сведения, отнесенные к государственной тайне: сведения в военной области, экономики, науки и техники, сведения в области внешней политики и экономики; сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты. – Оператор не является лидером, занимаемым значительный объем отраслевого рынка
2.	Преступные группы (криминальные структуры)	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, в следующих случаях: – в открытых источниках опубликованы выявленные случаи (новости, статьи, журналистские расследования, интервью), подтверждающие причастность преступных групп (криминальных структур) к противоправной деятельности в отрасли, в которой работает организация; – имеются статистические данные о причастности преступных групп (криминальных структур) к каким-либо инцидентам в организации; – в открытых источниках опубликованы сведения об уголовных делах на бывших работников организации.	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
3.	Террористические, экстремистские группировки	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя при наличии в организации опасных производственных объектов и (или) объектов топливно-энергетического комплекса и (или) потенциально опасных объектов: совершение на объекте (территории) террористического акта может привести к гибели людей или причинению вреда здоровью, возможному материальному ущербу и ущербу	Источник не актуален для Системы Оператора, т.к. Оператором не эксплуатируются опасные производственные объекты, и (или) объекты топливно-энергетического комплекса и (или) потенциально опасные объекты

№ п/п	Источник угроз	Критерии	Комментарий
1	2	3	4
		окружающей среде в районе расположения объекта (территории)	
5.	Отдельные физические лица (хакеры)	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя при наличии физического подключения Системы к информационно-телекоммуникационным сетям международного информационного обмена, в т.ч. сети «Интернет», или любым другим сетям, имеющим такие подключения	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
6.	Конкурирующие организации	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, в следующих случаях: – загрузка производственных мощностей может составлять не 100% в зависимости от наличия конкурентных предложений на рынке по одному и тому же виду деятельности; – в открытых источниках опубликованы выявленные случаи (новости, статьи, журналистские расследования, интервью) злонамеренных действий со стороны конкурентов (предприятий той же отрасли и вида деятельности); – в аналитических отчетах федеральной антимонопольной службы имеются выводы о достаточном или высоком уровне конкуренции в отрасли.	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
7.	Разработчики программных, программно-аппаратных средств	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, в следующих случаях: – источник актуален при наличии в Системе нелицензионного программного обеспечения и (или) программного обеспечения с открытым исходным кодом. – источник актуален при наличии в составе Системы индивидуально разработанных программных продуктов, функционирующих в составе общесистемного, прикладного и специального ПО; – источник актуален при наличии в составе Системы иностранного ПО / ОС, разработчики которого не осуществляют техническую поддержку программного продукта на территории Российской Федерации	Источник не актуален для Системы Оператора, т.к. в составе Системы не применяются нелицензионные программные продукты, программные продукты иностранного производства, разработчики которых не осуществляют техническую поддержку программного продукта на территории Российской Федерации, а также индивидуальные программные разработки
8.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя в случае, если подрядные организации имеют прямой физический или удаленный доступ к техническим средствам и (или) программно-аппаратным средствам, применяемым в Системе	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
9.	Поставщики вычислительных услуг, услуг связи		Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
10.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных		Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и

№ п/п	Источник угроз	Критерии	Комментарий
1	2	3	4
	видов работ		возможным негативным последствиям
11.	Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т.д.)	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, по умолчанию, т. к. по общемировой статистике не менее 50% инцидентов происходят по вине или с участием работников организации. При этом с учетом мотивации источника рассматриваются только антропогенные угрозы и угрозы, связанные с непреднамеренными действиями.	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям
12.	Авторизованные внутренние пользователи Системы		
13.	Администраторы программно-аппаратного комплекса Системы		
14.	Администраторы системы защиты информации Системы		
16.	Бывшие работники оператора	Источник подлежит рассмотрению в качестве потенциального актуального нарушителя, по умолчанию.	Источник может быть актуален для Системы Оператора при наличии соответствия целей видам риска (ущерба) и возможным негативным последствиям

Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий, приведенных в Разделе 3 Модели угроз, и видов ущерба от их реализации, приведена в таблице ниже (Таблица 6).

Таблица 6. Оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации.

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
1.	Бывшие работники оператора	+ (получение финансовой или иной материальной выгоды; моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия.)	+ (получение финансовой или иной материальной выгоды; моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия.)	● У1.1. Нарушение конфиденциальности (утечка) персональных данных; ● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий)	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды, получение конкурентных преимуществ)	● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); ● У2.5. Неспособность выполнения договорных обязательств; ● У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером;

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
				● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
3.	Отдельные физические лица (хакеры)	+ (любопытство или желание самореализации, подтверждение статуса, получение финансовой или иной материальной выгоды)	+ (любопытство или желание самореализации, подтверждение статуса, получение финансовой или иной материальной выгоды)	● У1.1. Нарушение конфиденциальности (утечка) персональных данных; ● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); ● У2.5. Неспособность выполнения договорных обязательств; ● У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий)	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды)	● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения,

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
				технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); ● У2.5. Неспособность выполнения договорных обязательств; ● У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
5.	Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды)	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды)	● У1.1. Нарушение конфиденциальности (утечка) персональных данных; ● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
6.	Преступные группы, - криминальные структуры, хакерские группы	+ (получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	+ (получение финансовой или иной материальной выгоды; желание самореализации (подтверждение статуса))	● У1.1. Нарушение конфиденциальности (утечка) персональных данных; ● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций;

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
				● У2.3. Простой информационной системы; ● У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств); ● У2.5. Неспособность выполнения договорных обязательств; ● У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
7.	Администраторы программно-аппаратного комплекса Системы	+ (получение финансовой или иной материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	+ (получение финансовой или иной материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
8.	Администраторы системы защиты	+ (получение финансовой или	+ (получение финансовой или	● У2.1. Необходимость дополнительных (незапланированных) затрат на

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
	информации Системы	иной материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	иной материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
9.	Поставщики вычислительных услуг, услуг связи	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды)	+ (непреднамеренные, неосторожные или неквалифицированные действия, получение финансовой или иной материальной выгоды)	● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
10.	Конкурирующие организации	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий)	+ (получение финансовой или иной материальной выгоды, получение конкурентных преимуществ)	● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств);

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	2	3	4	5
				● У2.5. Неспособность выполнения договорных обязательств; ● У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций); ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
11.	Авторизованные внутренние пользователи Системы	+ (получение финансовой или иной материальной выгоды; моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	+ (получение финансовой или иной материальной выгоды; моральное самоудовлетворение (в т. ч. профессиональное самоутверждение) без получения материальной выгоды; любопытство или желание самореализации (подтверждение статуса); месть за ранее совершенные действия; непреднамеренные, неосторожные или неквалифицированные действия)	● У1.1. Нарушение конфиденциальности (утечка) персональных данных; ● У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности; ● У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций; ● У2.3. Простой информационной системы; ● У2.5. Неспособность выполнения договорных обязательств; ● У2.7. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.); ● У2.8. Утрата доверия к Обществу; ● У2.9. Недополучение ожидаемой (прогнозируемой) прибыли; ● У2.10. Срыв запланированной сделки с партнером; ● У2.11. Потеря клиентов, поставщиков; ● У2.12. Потеря конкурентного преимущества; ● У2.13. Невозможность заключения договоров, соглашений; ● У2.14. Нарушение деловой репутации; ● У2.15. Снижение престижа; ● У2.16. Причинение имущественного ущерба.
12.	Разработчики программных, программно-аппаратных средств	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду	-

№ п/п	Виды нарушителей	Возможные цели реализации угроз безопасности информации		Соответствие целей видам риска (ущерба) и возможным негативным последствиям
		У1 Ущерб физическому лицу	У2 Ущерб Оператору Системы	
1	**2**	**3**	**4**	**5**
		несоответствия нарушителя критериям актуальности	несоответствия нарушителя критериям актуальности	
13.	Террористические, экстремистские группировки	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду несоответствия нарушителя критериям актуальности	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду несоответствия нарушителя критериям актуальности	-
14.	Специальные службы иностранных государств или блоков государств, в т. ч. иностранные технические разведки	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду несоответствия нарушителя критериям актуальности	- Отсутствуют цели реализации УБИ (причины деструктивных воздействий) ввиду несоответствия нарушителя критериям актуальности	-

5.3. Субъекты, не рассматриваемые в качестве потенциального нарушителя

5.3.1. Внешние нарушители

В связи с данными, приведенными в Таблицах Таблица 3 – Таблица 6, в дальнейшем при моделировании угроз не подлежат рассмотрению в качестве потенциальных нарушителей следующие категории субъектов (внешних нарушителей):

- Террористические, экстремистские группировки;
- Специальные службы иностранных государств или блоков государств, в т. ч. иностранные технические разведки.

5.3.2. Внутренние нарушители

В связи с данными, приведенными в Таблицах Таблица 3 – Таблица 6, в дальнейшем при моделировании угроз не подлежат рассмотрению в качестве потенциальных нарушителей следующие категории субъектов (внутренних нарушителей):

- Разработчики программных, программно-аппаратных средств.

5.4. Определение наиболее вероятных нарушителей ИБ

С учётом приведенных выше предположений о возможностях потенциальных нарушителей в качестве наиболее вероятных источников УБИ целесообразно рассматривать:

1. Внешний нарушитель:

- Бывшие работники оператора;
- Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- Отдельные физические лица (хакеры);
- Преступные группы, - криминальные структуры, хакерские группы;
- Конкурирующие организации.

2. Внутренний нарушитель:

- Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.);
- Администраторы программно-аппаратного комплекса Системы;
- Администраторы системы защиты информации Системы;
- Поставщики вычислительных услуг, услуг связи;
- Авторизованные внутренние пользователи Системы.

В дальнейшем необходимо учитывать, что возможности внешнего нарушителя весьма ограничены особенностями конфигурации ЛВС в целом, и Системы, в частности.

Сговор внешнего нарушителя с внутренним непривилегированным пользователем Системы **признается возможным.** К внутренним непривилегированным пользователям относятся следующие категории:

- Авторизованные внутренние пользователи Системы;
- Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.).

В таблице ниже приведены результаты определения потенциальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности, в соответствии с целями реализации угроз безопасности информации, определенными в настоящем документе.

Таблица 7. Результаты определения потенциальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности.

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	2	3	4	5
У1	●У1.1. Нарушение конфиденциальности (утечка) персональных данных	Бывшие работники оператора	Внешний	Н1
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
У2	●У2.1. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.2. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.3. Простой информационной системы	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	2	3	4	5
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Администраторы системы защиты информации Системы	Внутренний	H2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	H2
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2
		Конкурирующие организации	Внешний	H2
		Авторизованные внутренние пользователи Системы	Внутренний	H1
	●У2.4. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств)	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Конкурирующие организации	Внешний	H2
	●У2.5. Неспособность выполнения договорных обязательств	Бывшие работники оператора	Внешний	H1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Администраторы системы защиты информации Системы	Внутренний	H2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	H2
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2
		Конкурирующие организации	Внешний	H2
		Авторизованные внутренние пользователи Системы	Внутренний	H1
	●У2.6. Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций)	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Конкурирующие организации	Внешний	H2
	●У2.7. Утечка конфиденциальной	Бывшие работники оператора	Внешний	H1
		Отдельные физические лица (хакеры)	Внешний	H1

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	2	3	4	5
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Конкурирующие организации	Внешний	H2
		Авторизованные внутренние пользователи Системы	Внутренний	H1
	●У2.8. Утрата доверия к Обществу	Бывшие работники оператора	Внешний	H1
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Администраторы системы защиты информации Системы	Внутренний	H2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	H2
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2
		Авторизованные внутренние пользователи Системы	Внутренний	H1
	●У2.9. Недополучение ожидаемой (прогнозируемой) прибыли	Бывшие работники оператора	Внешний	H1
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Администраторы системы защиты информации Системы	Внутренний	H2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	H2
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2
		Конкурирующие организации	Внешний	H2
		Авторизованные внутренние пользователи Системы	Внутренний	H1
	●У2.10. Срыв запланированной сделки с партнером	Бывшие работники оператора	Внешний	H1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	H2
		Отдельные физические лица (хакеры)	Внешний	H1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	H2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	H1
		Администраторы системы защиты информации Системы	Внутренний	H2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	H2
		Поставщики вычислительных услуг, услуг связи	Внутренний	H2

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	2	3	4	5
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.11. Потеря клиентов, поставщиков	Бывшие работники оператора	Внешний	Н1
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.12. Потеря конкурентного преимущества	Бывшие работники оператора	Внешний	Н1
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.13. Невозможность заключения договоров, соглашений	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.14. Нарушение деловой репутации	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2

№ п/п	Виды риска (ущерба) и возможные негативные последствия	Виды актуального нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	2	3	4	5
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.15. Снижение престижа	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1
	●У2.16. Причинение имущественного ущерба	Бывшие работники оператора	Внешний	Н1
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н1
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Преступные группы, - криминальные структуры, хакерские группы	Внешний	Н2
		Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	Н1
		Администраторы системы защиты информации Системы	Внутренний	Н2
		Администраторы программно-аппаратного комплекса Системы	Внутренний	Н2
		Поставщики вычислительных услуг, услуг связи	Внутренний	Н2
		Конкурирующие организации	Внешний	Н2
		Авторизованные внутренние пользователи Системы	Внутренний	Н1

Перечень актуальных нарушителей безопасности информации с указанием уровня возможностей и потенциала приведен в таблице ниже.

Таблица 8. Актуальные нарушители безопасности информации.

№ п/п	Виды нарушителей	Уровень возможностей нарушителей	Потенциал	Категория нарушителя
1	**2**	**3**	**4**	**5**
1.	Бывшие работники оператора	Нарушитель, обладающий базовыми возможностями (Н1)	Низкий	Внешний
2.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Нарушитель, обладающий базовыми возможностями (Н1)	Низкий	Внешний
3.	Отдельные физические лица (хакеры)	Нарушитель, обладающий базовыми возможностями (Н1)	Низкий	Внешний
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внутренний
5.	Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Нарушитель, обладающий базовыми возможностями (Н1)	Низкий	Внутренний
6.	Преступные группы, - криминальные структуры, хакерские группы	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внешний
7.	Администраторы программно-аппаратного комплекса Системы	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внутренний
8.	Администраторы системы защиты информации Системы	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внутренний
9.	Поставщики вычислительных услуг, услуг связи	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внутренний
10.	Конкурирующие организации	Нарушитель, обладающий базовыми повышенными возможностями (Н2)	Средний	Внешний
11.	Авторизованные внутренние пользователи Системы	Нарушитель, обладающий базовыми возможностями (Н1)	Низкий	Внутренний

Таким образом, и с учетом возможности сговора внешнего нарушителя с внутренним непривилегированными пользователем в ходе анализа было определено, что актуальными являются **внешние и внутренние нарушители с низким и средним потенциалом**.

6 ОЦЕНКА СПОСОБОВ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1. **Способы реализации (возникновения) угроз безопасности информации**

При определении основных способов реализации УБИ в отношении ресурсов Системы, учитывались необходимость обеспечения информационной безопасности на всех этапах жизненного цикла Системы, компонентов, условий функционирования Системы, а также предположений о вероятных нарушителях, негативных последствиях, объектах и видах воздействия.

Рассмотрению подлежат следующие типы способов реализации угроз информационной безопасности Системы, подлежащие уточнению в соответствии со структурно-функциональными характеристиками, а также актуальными источниками угроз безопасности информации Системы:

- использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);
- внедрение вредоносного программного обеспечения;
- использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
- установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;
- формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
- ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств;
- несанкционированный доступ к защищаемой информации с использованием штатных средств Системы и недостатков механизмов разграничения доступа;
- несанкционированный доступ к защищаемой информации из ЛВС или защищённых сетей, имеющих доступ к ЛВС (из сетей внешнего взаимодействия);
- маскировка под администратора Системы, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых Системе;
- осуществление прямого хищения (утраты) элементов Системы, носителей информации и производственных отходов (распечаток, списанных носителей);
- компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых Системе;

– методы социальной инженерии для получения сведений о Системе, способствующих созданию благоприятных условий для применения других методов;

– использование оставленных без присмотра незаблокированных средств администрирования Системы и АРМ администраторов;

– сбои и отказы программно-технических компонентов Системы;

– внесение неисправностей, уничтожение технических и программно-технических компонентов Системы путем непосредственного физического воздействия;

– запуск нештатных режимов функционирования ОТСС Системы;

– осуществление несанкционированного доступа к информации через различные носители информации и элементы средств вычислительной техники, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) могут оказаться за пределами контролируемой зоны.

Основными способами реализации (возникновения) УБИ для Системы являются:

– С1: использование уязвимостей (уязвимостей кода (ПО), уязвимостей архитектуры и конфигурации Системы, а также организационных и многофакторных уязвимостей);

– С2: внедрение вредоносного ПО;

– С3: использование недекларированных возможностей ПО и (или) программно-аппаратных средств;

– С4: установка программных и (или) программно-аппаратных закладок в ПО и (или) программно-аппаратные средства;

– С5: формирование и использование скрытых каналов (по времени, по памяти) для передачи защищаемой информации;

– С6: инвазивные способы доступа к защищаемой информации, а также аппаратно-программному комплексу;

– С7: нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

– С8: ошибочные действия в ходе создания и эксплуатации Системы, в том числе при установке, настройке программных и программно-аппаратных средств;

– С9: несанкционированный доступ к защищаемой информации с использованием штатных средств Системы и недостатков механизмов разграничения доступа;

– С10: несанкционированный доступ к защищаемой информации из ЛВС или защищённых сетей, имеющих доступ к ЛВС (из сетей внешнего взаимодействия);

– С11: маскировка под администратора Системы, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых Системе;

– С12: осуществление прямого хищения (утраты) элементов Системы, носителей информации и производственных отходов (распечаток, списанных носителей);

– С13: компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых Системе;

– С14: методы социальной инженерии для получения сведений о Системе, способствующих созданию благоприятных условий для применения других методов;

– С15: использование оставленных без присмотра незаблокированных средств администрирования Системы и АРМ администраторов;

– С16: сбои и отказы программно-технических компонентов Системы;

– С17: внесение неисправностей, уничтожение технических и программно-технических компонентов Системы путем непосредственного физического воздействия;

– С18: запуск нештатных режимов функционирования ОТСС Системы;

– С19: осуществление несанкционированного доступа к информации через различные носители информации и элементы средств вычислительной техники, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) могут оказаться за пределами контролируемой зоны.

6.2. **Интерфейсы объектов воздействия**

Условием, позволяющим нарушителям использовать способы реализации УБИ, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия и возможностям доступа:

– И1: внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями;

– И2: внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами Системы, имеющими внешние сетевые интерфейсы (проводные);

– И3: интерфейсы для пользователей (проводные пользовательские интерфейсы доступа, веб-интерфейс, др.);

– И4: интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

– И5: интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов Системы;

– И6: возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам Системы;

– И7: интерфейс удаленного администрирования компонентов Системы, расположенных на базе информационно-телекоммуникационной инфраструктуры центра обработки данных;

– И8: каналы связи с внешними информационно-телекоммуникационными системами;

– И9: механизмы обновлений программного обеспечения компонентов Системы;

– И10: пользователи.

Определение интерфейсов объектов воздействия основывается на предположениях об источниках угроз безопасности информации, и доступных им видах воздействия.

6.2.1. **Внутренние интерфейсы доступа к объектам защиты**

К внутренним интерфейсам доступа к объектам защиты Системы относятся:

– И2: внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами Системы, имеющими внешние сетевые интерфейсы (проводные);

– И3: интерфейсы для пользователей (проводные пользовательские интерфейсы доступа, веб-интерфейс, др.);

– И4: интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

– И5: интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов Системы;

– И6: возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам Системы;

– И10: пользователи.

6.2.2. **Внешние интерфейсы доступа к объектам защиты**

К внешним интерфейсам доступа к объектам защиты Системы относятся:

– И1: внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями;

– И7: интерфейс удаленного администрирования компонентов Системы, расположенных на базе информационно-телекоммуникационной инфраструктуры центра обработки данных;

– И8: каналы связи с внешними информационно-телекоммуникационными системами;

– И9: механизмы обновлений программного обеспечения компонентов Системы.

Эксплуатация методов социальной инженерии в отношении привилегированных пользователей не рассматривается в связи с высокой квалификацией специалистов и мерами физической защиты программно-аппаратного комплекса.

Таблица 9. Возможные способы реализации угроз в соответствии с актуальными нарушителями безопасности информации.

№ п/п	Актуальный источник УБИ	Категория нарушителя	Способы реализации УБИ	Доступные интерфейсы
1	2	3	4	5
1.	Преступные группы (криминальные структуры)	Внешний	С1, С2, С3, С5, С12, С14, С16, С19	И1, И6, И8, И9, И10
2.	Отдельные физические лица (хакеры)	Внешний	С1, С2, С3, С5, С12, С14, С16	И1, И8, И9, И10
3.	Лица, привлекаемые для установки, наладки, монтажа, обслуживания инфраструктуры, пусконаладочных и иных видов работ (подрядчики)	Внутренний	С1, С2, С3, С5, С6, С7, С8, С15, С17	И1, И2, И5, И7, И8, И9
4.	Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний	С2, С5, С6, С9, С10, С13, С15, С16, С17	И2, И4
5.	Администраторы системы защиты информации Системы	Внутренний	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18	И2, И3, И5, И7, И9
6.	Администраторы программно-аппаратного комплекса Системы	Внутренний	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18	И2, И3, И5, И7, И9
7.	Авторизованные внутренние пользователи Системы	Внутренний	С1, С8, С9, С10, С11, С12, С13, С15, С16	И1, И2, И3
8.	Бывшие работники оператора	Внешний	С1, С2, С3, С5, С16	И1, И8, И9, И10
9.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	С1, С2, С3, С6, С7, С8, С16, С18	И6
10.	Поставщики вычислительных услуг, услуг связи	Внутренний	С1, С2, С3, С5, С16, С17	И1, И2, И4, И7
11.	Конкурирующие организации	Внешний	С1, С2, С3, С5, С12, С16, С19	И1, И8, И9, И10

В соответствии с предположениями, приведенными в Разделах 3 – 5 настоящего документа, и с учетом возможного сговора внутреннего и внешнего нарушителя, в Таблице ниже сформированы возможные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности (Таблица 10).

Таблица 10. Способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
1.	Преступные группы (криминальные структуры), хакерские группы	Внешний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И10	С1, С2, С3, С5, С12, С14, С19
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И8, И9, И10	С1, С2, С3, С5, С12, С14, С19
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И8, И9, И10	С1, С2, С3, С14
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И8, И9	С1, С2, С3, С14, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С12, С19
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И8, И9	С1, С2, С3, С14, С16, С19
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И6, И9, И10	С1, С2, С3, С14, С16, С19
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				(нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
2.	Отдельные физические лица (хакеры)	Внешний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И10	С1, С2, С3, С5, С12, С14
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И9, И10	С1, С2, С3, С5, С12, С14
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И9, И10	С1, С2, С3, С14
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И8, И9	С1, С2, С3, С14, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С12
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения	И1, И8, И9, И10	С1, С2, С3, С14, С16

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			(сетевое оборудование)	сетевых атак)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И9, И10	С1, С2, С3, С14, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
3.	Лица, привлекаемые для установки, наладки, монтажа, обслуживания инфраструктуры, пусконаладочных и иных видов работ (подрядчики)	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И5, И7, И8	С1, С2, С5, С8, С18, С19
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И5, И7, И8	С1, С2, С8, С18, С19
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С16, С17,

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С16, С17, С18
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С16, С17, С18
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С16, С17, С18
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С16, С17, С18
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2, И5, И7, И8	С1, С2, С6, С7, С8, С15, С17, С18
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И1, И4	С1, С2, С3, С19
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И1, И2, И5, И7	С1, С2, С3, С6, С7, С8, С17, С18
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2, И5, И7, И9	С1, С2, С3, С6, С7, С8, С17, С18
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И8	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				(нарушение целостности)		
4.	Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.)	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И4	С1, С2, С3
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И4	С1, С2, С3, С5, С6, С7, С8, С15, С17
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2	С2, С5

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
5.	Администраторы системы защиты информации Системы	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3	С1, С2, С3, С5, С6, С9, С10, С12
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И2, И3	С1, С2, С3, С5, С6, С9, С10, С12
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И2, И3	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3, И5	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И2, И3	С1, С2, С3, С5, С6, С8, С9, С10, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И2, И3	С1, С2, С3, С5, С6, С8, С9, С10, С16
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С8, С9, С10, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И4, И8	С1, С2, С3, С8, С12
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И4, И8	С1, С2, С3, С8, С12
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И4, И8, И9	С1, С2, С3, С8, С12
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
6.	Администраторы программно-аппаратного комплекса Системы	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3, И5, И7	С1, С2, С3, С5, С6, С9, С10, С12
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С9, С10, С12
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И2, И3, И5, И7, И9	С1, С2, С3, С5, С6, С7, С8, С9, С10, С12, С16, С18
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И2, И3	С1, С2, С3, С5, С6, С7, С8, С9, С10,
				Несанкционированная модификация, подмена, искажение защищаемой		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				информации, системных, конфигурационным иных служебных данных (нарушение целостности)		С12, С16, С18
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И4, И8	С1, С2, С3, С8, С12
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И4, И8, И9	С1, С2, С3, С8, С12
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И4, И8, И9	С1, С2, С3, С8, С12
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И2, И3, И7	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				ПЕРЕХВАТ ЗАЩИЩАЕМОЙ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ЛИНИЯМ СВЯЗИ		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
7.	Авторизованные внутренние пользователи Системы	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И3	С1, С8, С9, С10, С11
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И3	С1, С8, С10, С13, С15
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И3	С1, С8, С10, С13, С15
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И3	С1, С8, С10, С13, С15
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И2, И3	С1, С8, С10, С13, С15
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	-	-	-
			Среда виртуализации (Гипервизор)	-	-	-
			Средства защиты информации	-	-	-
			Несъемные носители информации	-	-	-
			Аппаратное обеспечение (сетевое оборудование)	-	-	-
			Микропрограммное обеспечение (BIOS / UEFI)	-	-	-
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И3	С1, С8, С10, С13, С15
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
8.	Бывшие работники оператора	Внешний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И10	С1, С2, С3, С5
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				(нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И9, И10	С1, С2, С3, С5
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И9, И10	С1, С2, С3
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С16
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные	-	-	-

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			машины (образы виртуальных машин)			
			Среда виртуализации (Гипервизор)	-	-	-
			Средства защиты информации	-	-	-
			Несъемные носители информации	-	-	-
			Аппаратное обеспечение (сетевое оборудование)	-	-	-
			Микропрограммное обеспечение (BIOS / UEFI)	-	-	-
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
9.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И6	С1, С2, С3, С6
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И6	С1, С2, С3, С6, С7, С8, С16

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И6	С1, С2, С3, С6, С7, С8, С16
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И6	С1, С2, С3, С6, С7, С8, С16
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И6	С1, С2, С3, С6, С7, С8, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И6	С1, С2, С3, С6, С7, С8, С16
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И6	С1, С2, С3, С6, С7, С8, С16
				Отказ в обслуживании компонентов (нарушение доступности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И6	С1, С2, С3, С6, С7, С8, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И6	С6, С7, С8, С16, С19
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И6	С6, С7, С8, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И6	С6, С7, С8, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	-	-	-
10.	Поставщики вычислительных услуг, услуг связи	Внутренний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И4, И7	С1, С2, С3, С5
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				(нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И4, И7	С1, С2, С3, С5, С16, С17
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И2, И4, И7	С1, С2, С3, С5, С16, С17
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2, И4, И7	С1, С2, С3, С5, С16, С17
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И2, И4, И7	С1, С2, С3, С5, С16, С17
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И2, И4, И7	С1, С2, С3, С16, С17
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2, И4, И7	С1, С2, С3, С16, С17
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2, И4, И7	С1, С2, С3, С16, С17
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И1, И2, И4	С1, С2, С3, С16, С17
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И1, И2	С1, С2, С3, С16, С17
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И2	С1, С2, С3, С16, С17
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И2	С1, С2, С3, С5

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
11.	Конкурирующие организации	Внешний нарушитель	Защищаемые информационные ресурсы ограниченного доступа	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И10	С1, С2, С3, С5, С12, С14, С19
				Утечка защищаемой информации, путем НСД к технологическим журналам программного комплекса Системы		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Реестр	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И8, И9, И10	С1, С2, С3, С5, С12, С14, С19
			Прикладное программное обеспечение	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)	И1, И8, И9, И10	С1, С2, С3, С14
				Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе журналов и БД Системы (нарушение конфиденциальности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)		
			Система управления базой данных (СУБД)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
			Системное программное обеспечение (ВМ)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Виртуальные машины (образы виртуальных машин)	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С14, С16
				Несанкционированный доступ к защищаемой информации, содержащейся в составе объектов файловой системы (нарушение конфиденциальности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Среда виртуализации (Гипервизор)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И1, И8, И9	С1, С2, С3, С14, С16
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Средства защиты информации	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И8, И9	С1, С2, С3, С14, С16
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
				Отказ в обслуживании компонентов (нарушение доступности)		
			Несъемные носители информации	Несанкционированный доступ к информации субъектов ПДн, содержащейся в составе объектов файловой системы и БД (нарушение конфиденциальности)	И1, И8, И9	С1, С2, С3, С12, С19
				Утечка защищаемой информации, путем НСД к носителям информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Аппаратное обеспечение (сетевое оборудование)	Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)	И8, И9	С1, С2, С3, С14, С16, С19
				Отказ в обслуживании компонентов (нарушение доступности)		
				НСД к защищаемой информации путем эксплуатации уязвимостей аппаратного		

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Виды воздействия	Доступные интерфейсы	Способы реализации
1	2	3	4	5	6	7
				обеспечения, сетевого оборудования		
				Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Микропрограммное обеспечение (BIOS / UEFI)	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передача и хранение информации	И6, И9, И10	С1, С2, С3, С14, С16, С19
				Отказ в обслуживании компонентов (нарушение доступности)		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		
			Каналы связи (сетевой трафик)	Утечка (перехват) защищаемой информации или отдельных данных (нарушение конфиденциальности)	И1, И8	С1, С2, С3, С5
				Несанкционированное использование каналов связи для проведение сетевых атак (участие в DDoS атаках, сканирование удаленных узлов, эксплуатация уязвимостей узлов внутреннего сетевого взаимодействия, пр.)		
				Отказ в обслуживании компонентов (нарушение доступности)		
				Получение несанкционированного доступа к техническим средствам и использования их для майнинга криптовалют, участия в ботнетах (проведения сетевых атак)		
				ПЕРЕХВАТ ЗАЩИЩАЕМОЙ ТЕХНОЛОГИЧЕСКОЙ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ЛИНИЯМ СВЯЗИ		
				Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационным иных служебных данных (нарушение целостности)		

7 ФОРМИРОВАНИЕ ПЕРЕЧНЯ ТАКТИК И ТЕХНИК

В ходе определения сценариев реализации угроз безопасности информации определяются применимые основные тактики и соответствующие им техники, используемые для построения сценариев реализации угроз безопасности информации.

Исходными данными для определения формирования перечня тактик и соответствующих им техник является описание архитектуры Системы, технологии обработки информационных ресурсов, а также структурно-функциональные характеристики Системы, приведенные в Разделе 2.

Перечень актуальных тактик и техник для Системы приведен в Приложении 1 к настоящему документу.

8 ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В ходе оценки угроз безопасности информации определяются возможные угрозы безопасности информации и оценивается их актуальность для Системы.

Вопросы защиты от угроз, не связанных с деятельностью человека, угроз социально-политического и техногенного характера не являются предметом для рассмотрения в рамках данной модели, поскольку масштаб их возможного деструктивного воздействия, превосходит возможности системы защиты информации Системы.

Для Системы необходимо обеспечить *конфиденциальность, целостность, доступность* объектов воздействия, определенных в настоящей Модели угроз, в соответствии с БДУ ФСТЭК России.

Таблица 11. Перечень рассматриваемых угроз безопасности информации и оценка их актуальности

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
УБИ.006	Угроза внедрения кода или данных	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями или автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.), а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов. Данная угроза обусловлена наличием уязвимостей программного обеспечения, а также слабостями мер антивирусной защиты. Реализация данной угрозы возможна в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников, или при наличии у него привилегий установки программного обеспечения.	Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	C2, C3	T1.1, T1.3, T1.4, T1.5 T1.11, T1.12, T1.15, T1.16 T2.6, T2.7, T2.8, T2.10, T2.11 T3.1, T3.5, T3.7, T3.10 T4.2, T4.3, T4.5 T5.1, T5.2 T6.6, T6.8 T7.9, T7.10, T7.12, T7.23 T10.11	**Актуальная**
УБИ.010	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора,	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины	C1, C2, C3, C5, C6, C8, C9, C10, C11, C15, C16, C18	T1.1, T1.11, T1.12, T1.15 T2.7, T2.8, T2.9 T3.1, T3.6, T3.7, T3.10, T3.14, T3.15, T3.16 T4.1, T4.2, T4.3, T4.4, T4.5, T4.7 T5.1, T5.2, T5.5, T5.11, T6.1, T6.2, T6.3, T6.4, T6.5, T6.6, T6.7, T6.8,	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		реализующего функцию изолированной программной среды для функционирующих в ней программ, а также слабостями инструкций аппаратной поддержки виртуализации на уровне процессора. Реализация данной угрозы приводит не только к компрометации гипервизора, но и запущенных в созданной им виртуальной среде средств защиты, а, следовательно, к их неспособности выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора.				Т6.9 Т7.1, Т7.2, Т7.3, Т7.4, Т7.6, Т7.8, Т7.10, Т7.11, Т7.12, Т7.13, Т7.14, Т7.15, Т7.16, Т7.23, Т7.26 Т8.1, Т8.2, Т8.3, Т8.4, Т8.7, Т8.8 Т9.1, Т9.2, Т9.10, Т9.14 Т10.7, Т10.8, Т10.9, Т10.10, Т10.11	
УБИ.017	Угроза доступа/перехвата/ изменения HTTP cookies	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя). Данная угроза обусловлена слабостями мер защиты cookies-файлов: отсутствием проверки вводимых данных со стороны сетевой службы, использующей cookies-файлы, а также отсутствием шифрования при передаче cookies-файлов. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к cookies-файлам и отсутствии проверки целостности	Внешний нарушитель с низким потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	С1, С2, С3, С5, С8, С10, С11	Т1.3, Т1.4, Т1.5, Т1.8, Т1.11, Т2.5, Т2.13 Т4.2 Т10.1	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		их значений со стороны дискредитируемого приложения					
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	C1, C2, C3, C5, C6, C8, C9, C10, C11, C15, C16, C18	Угроза является техникой реализации T6.8	**Актуальная**
УБИ.042	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	Внешний нарушитель со средним потенциалом	Сетевой узел, сетевое программное обеспечение	C2, C3, C8, C14	T3.3 T5.3 T7.9, T7.10, T7.17 T8.7 T10.4	**Актуальная**
УБИ.054	Угроза недобросовестного	Угроза заключается в возможности раскрытия или повреждения	Внешний нарушитель с	Информационная система, сервер,	C8, C16	T2.3, T2.4, T2.5, T2.6, T2.7, T2.9, T2.10, T2.11	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
	исполнения обязательств поставщиками облачных услуг	целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения требований к уровню качества (уровню доступности) предоставляемых потребителям облачных услуг доступа к их программам или иммигрированным в облако информационным системам. Данная угроза обусловлена невозможностью непосредственного контроля над действиями сотрудников поставщика облачных услуг со стороны их потребителей. Реализация данной угрозы возможна в случаях халатности со стороны сотрудников поставщика облачных услуг, недостаточности должностных и иных инструкций данных сотрудников, недостаточности мер по менеджменту и обеспечению безопасности облачных услуг и т.д.	низким потенциалом	носитель информации, метаданные, объекты файловой системы		Т3.2, Т3.3, Т3.4, Т3.5, Т3.7, Т3.10, Т3.11, Т3.12, Т3.13, Т3.14, Т3.15, Т3.16 Т4.2, Т4.3, Т4.4, Т4.5, Т4.7 Т5.1, Т5.2 Т6.6, Т6.8, Т6.9 Т7.9, Т7.12, Т7.14, Т7.15, Т7.16 Т10.1, Т10.2, Т10.7, Т10.8, Т10.9	
УБИ.063	Угроза некорректного использования функционала программного обеспечения	Угроза заключается в возможности использования декларированных возможностей программных и аппаратных средств определённым (нестандартным, некорректным) способом с целью деструктивного воздействия на информационную систему и обрабатываемую ею информацию. Данная угроза связана со слабостями механизма обработки данных и команд, вводимых пользователями. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к программным и аппаратным средствам	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение	С1, С2, С3, С5, С7	Т2.3, Т2.4, Т2.5, Т2.6, Т2.8, Т2.10, Т2.11 Т6.1, Т6.2, Т6.4, Т6.6, Т6.8 Т10.2, Т10.3	**Актуальная**
УБИ.068	Угроза неправомерного/ некорректного	Угроза заключается в возможности осуществления нарушителем	Внутренний нарушитель со	Системное программное	С1, С2, С3, С5, С6, С7, С8	Т3.12, Т3.13 Т10.2, Т10.3	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
	использования интерфейса взаимодействия с приложением	деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API). Данная угроза обусловлена наличием слабостей в механизме проверки входных данных и команд API, используемого программным обеспечением. Реализация данной угрозы возможна в условиях наличия у нарушителя доступа к API и отсутствия у дискредитируемого приложения механизма проверки вводимых данных и команд	средним потенциалом Внешний нарушитель со средним потенциалом	обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр			
УБИ.069	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	Внешний нарушитель с низким потенциалом	Сетевой трафик	C1, C2, C3, C5, C8, C10, C11	T1.3, T1.4 T2.3, T2.4, T2.5, T2.13 T8.5 T10.7, T10.8, T10.9	**Актуальная**
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём	Внутренний нарушитель со средним потенциалом Внешний	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные	C1, C2, C3, C5, C8, C10, C11	T1.3, T1.4, T1.7 T2.3, T2.4, T2.5, T2.6, T2.9, T2.10 T4.1, T4.2 T5.2 T6.2, T6.8	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
	оборудованию из физической и (или) виртуальной сети	эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования. Данная угроза обусловлена ограниченностью функциональных возможностей (наличием слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	нарушитель со средним потенциалом	устройства		T7.1 T10.2	
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	Угроза заключается в возможности извлечения паролей из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации. Данная угроза обусловлена наличием слабостей мер разграничения доступа к защищаемой информации. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	C1, C2, C3, C5, C6, C8, C9, C10, C11, C14, C15, C16, C18	T1.9 T2.10 T3.3 T5.3 T6.1, T6.2, T6.8 T9.3, T9.13 T10.1	**Актуальная**
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ	Внутренний нарушитель со средним потенциалом Внешний нарушитель со	Гипервизор	C1, C2, C3, C5, C6, C8, C9, C10, C11, C15, C16, C18	T2.3, T2.4, T2.5 T6.1, T6.2, T6.8 T10.2, T10.11	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: — наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; — наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью	средним потенциалом				
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Виртуальная машина	C1, C2, C3, C5, C6, C8, C9, C10, C11, C15, C16, C18	T1.4, T1.5, T1.7 T2.3, T2.4, T2.5 T7.1	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия					
УБИ.086	Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или специальных программных средств. Данная угроза обусловлена наличием слабостей мер разграничения доступа к информации аутентификации. Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учётной записью дискредитированного пользователя	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Системное программное обеспечение, объекты файловой системы, учётные данные пользователя, реестр	C1, C2, C3, C5, C6, C8, C9, C10, C11, C14, C15, C16, C18	T1.8, T1.9 T2.8, T2.10, T2.11 T4.1 T7.1 T10.1	**Актуальная**
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации	Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). Данная угроза обусловлена в случае некорректных значений параметров конфигурации	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Системное программное обеспечение, сетевое программное обеспечение	C1, C8	Угроза является техникой реализации T6.7	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		средств аутентификации и/или отсутствием контроля входных данных. Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации					
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном (иногда в активном) режиме (т.е. «прослушивать сетевой трафик») для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым (скрытным) получателем перехватываемых данных. Кроме того, нарушитель может проводить исследования других типов потоков данных, например, радиосигналов. Данная угроза обусловлена слабостями механизмов сетевого взаимодействия, предоставляющими сторонним пользователям открытые данные о дискредитируемой системе, а также ошибками конфигурации сетевого программного обеспечения. Реализация данной угрозы возможна в следующих условиях: — наличие у нарушителя доступа к дискредитируемой вычислительную сети; неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока	Внешний нарушитель с низким потенциалом	Сетевой узел, сетевой трафик	C1, C2, C3, C5, C9, C10, C11	T1.3, T1.4, T1.7 T2.3, T2.4, T2.13 T9.7	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		данных					
УБИ.127	Угроза подмены действия пользователя путём обмана	Угроза заключается в возможности нарушителя выполнения неправомерных действий в системе от имени другого пользователя с помощью методов социальной инженерии (обмана пользователя, навязывание ложных убеждений) или технических методов (использование прозрачных кнопок, подмена надписей на элементах управления и др.). Данная угроза обусловлена слабостями интерфейса взаимодействия с пользователем или ошибками пользователя. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя прав на проведение нужных от него нарушителю операций	Внешний нарушитель со средним потенциалом	Прикладное программное обеспечение, сетевое программное обеспечение	C14	T2.8	**Актуальная**
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой. Данная угроза обусловлена тем, что для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с ограниченностью скорости обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку	Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом	Информационная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	C1, C2, C3, C16	Угроза является техникой реализации T10.7	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы					
УБИ.165	Угроза включения в проект недостоверно испытанных компонентов	Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др. Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированной и др.	Внутренний нарушитель со средним потенциалом	Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры	C1, C2, C3, C5, C6, C7, C8, C16, C18	Для угрозы отсутствует тактика и техника	**Актуальная**
УБИ.175	Угроза «фишинга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) зайти на поддельный сайт	Внешний нарушитель с низким потенциалом	Рабочая станция, сетевое программное обеспечение, сетевой трафик	C14	В соответствии с технологическим процессом, угроза признана неприменимой.	**Актуальная**

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).	Описание угрозы	Источники угрозы	Объект воздействия	Сценарии реализации угроз		Актуальность угрозы
					Способы реализации	Тактики и техники	
1	2	3	4	5	6	7	8
		(выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию или открыть заражённое вложение в письме. Данная угроза обусловлена недостаточностью знаний пользователей о методах и средствах «фишинга». Реализация данной угрозы возможна при условии наличия у нарушителя: — сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; — средств создания и запуска поддельного сайта; — сведений о контактах пользователя с доверенной организацией (номер телефона, адрес электронной почты и др.). Для убеждения пользователя раскрыть информацию ограниченного доступа (или открыть вложение в письмо) наиболее часто используются поддельные письма от администрации какой-либо организации, с которой взаимодействует пользователь (например, банк)					

9. СОВОКУПНОСТЬ ПРЕДПОЛОЖЕНИЙ О ВОЗМОЖНОСТЯХ, КОТОРЫЕ МОГУТ И ИСПОЛЬЗОВАТЬСЯ ПРИ СОЗДАНИИ СПОСОБОВ, ПОДГОТОВКЕ И ПРОВЕДЕНИИ АТАК НА ОБЪЕКТ ИНФОРМАТИЗАЦИИ

9.1. Обобщённые возможности нарушителя применительно к СКЗИ

С учётом предположений о характеристиках и возможностях рассматриваемых нарушителей безопасности информации были сформированы суждения об обобщённых возможностях нарушителей применительно к СКЗИ и среде их функционирования.

Таблица 12. Сведения об обобщённых возможностях нарушителя применительно к СКЗИ.

Тип нарушителя	Обобщённые возможности нарушителя	Тип нарушителя применительно к СКЗИ
1	2	3
Бывшие работники оператора	– Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Н1
Авторизованные внутренние пользователи Системы		
Конкурирующие организации		
Отдельные физические лица (хакеры)		
Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т.д.)	– Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	Н2
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	– Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Н3
Лица, привлекаемые для установки, наладки, монтажа, обслуживания инфраструктуры, пусконаладочных и иных видов работ (подрядчики)		
Администраторы системы защиты информации Системы		
Администраторы программно-аппаратного комплекса Системы		
Преступные группы, - криминальные структуры, хакерские группы	– Возможность привлекать специалистов, имеющих, опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов, линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ). – Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения).	Н4, Н5
Террористические группировки, экстремистские группировки		
Разработчики программных, программно-аппаратных средств		
Специальные службы иностранных государств или блоков государств, в т.ч. иностранные технические разведки	– Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ.	Н6

С учётом сведений, приведенных в Разделе 5 Модели угроз, и предположений о возможностях потенциальных нарушителей, в качестве наиболее вероятных источников УБИ, в отношении СКЗИ и среды функционирования СКЗИ, актуальными признаются следующие категории:

1. Внешний нарушитель:

- Бывшие работники оператора;
- Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- Отдельные физические лица (хакеры);
- Преступные группы, - криминальные структуры, хакерские группы;
- Конкурирующие организации.

2. Внутренний нарушитель:

- Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- Лица, обеспечивающие функционирование Системы или обеспечивающих систем управления (администрация, охрана, уборщики и т. д.);
- Администраторы программно-аппаратного комплекса Системы;
- Администраторы системы защиты информации Системы;
- Поставщики вычислительных услуг, услуг связи;
- Авторизованные внутренние пользователи Системы.

Возможность привлечения специалистов, имеющих опыт разработки и анализа СКЗИ, включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ и специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения, то для защиты информации в Системе (компонентов Системы) признана неактуальной.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе:

- по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров;
- контролю допуска физических лиц внутрь контролируемой зоны ЦОД, а также офисных помещений, из которых осуществляют подключения авторизованные пользователи Системы, и контролю за порядком проведения работ в пределах соответствующих КЗ, направленных на предотвращение и пресечение несанкционированных действий.

С учетом мер физической защиты, контрольно-пропускным режимом, работами по подбору и расстановке персонала, а также используемыми в Системе средствами защиты информации и мерами защиты от несанкционированного доступа, признаются актуальными внешние нарушители, не имеющие доступ в пределы контролируемой зоны, а также не имеющие непосредственного доступа к СКЗИ / среде функционирования СКЗИ:

- Преступные группы, - криминальные структуры, хакерские группы;
- Бывшие работники оператора;

- Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- Отдельные физические лица (хакеры).

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Отдельно отмечается, что по результатам моделирования угроз, угрозы, связанные с возможным деструктивным воздействием на микропрограммное обеспечение (BIOS/UEFI), а также аппаратный комплекс Системы признаются актуальными исключительно для компонентов Системы, не являющихся СКЗИ, либо средой их функционирования, а также в соответствии с Методическим документом ФСТЭК России «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России 05.02.2021 г. (Информационное сообщение ФСТЭК России от 15 февраля 2021г. №240/22/690)», при моделировании угроз безопасности информации Системы не учитывались меры защиты информации уже реализованные на объекте автоматизации, которые должны учитываться при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак такие, как:

– СКЗИ Системы предполагаются к размещению на базе информационно-телекоммуникационной инфраструктуры ЦОД, имеющей действующей Аттестат соответствия требованиям о защите информации. Сведения о выданном Аттестате соответствия требованиям о защите информации приведены в Разделе 2.7 настоящего документа;

– в составе комплекса средств защиты информации ЦОД применяются сертифицированные ФСТЭК России и ФСБ России, в части их касающейся;

– помещения размещения физических технических средств оборудованы системами контроля и управления доступом. Серверные стойки запираются и опечатываются ответственными лицами. В помещения допускаются работники ЦОД, в соответствии с перечнем допущенных лиц. Коридоры оборудованы системами видеонаблюдения. Бесконтрольное нахождение посторонних лиц, а также работников, имеющих доступ в помещения, но недопущенных к указанным стойкам, исключено;

– ВМ Системы оборудованы средствами антивирусной защиты информации, имеющими сертификаты ФСТЭК России и ФСБ России.

9.2. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, в соответствии с положениями Приказа ФСБ России от 10.07.2014 № 378

С учётом сведений, приведённых выше, можно сделать выводы об обобщённых возможностях источников атак.

Таблица 13. Оценка реализуемости возможностей источников атак.

№ п/п	Обобщенные возможности источников атак	Оценка реализуемости возможности	Примечание
1	2	3	4
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	+	-
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к АС, на которых реализованы СКЗИ и среда их функционирования	-	См. Таблица 14
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	-	См. Таблица 14
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	-	См. Таблица 14
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	-	См. Таблица 14
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	-	См. Таблица 14

Таблица 14. Обоснование неактуальности угроз.

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Факторы, нейтрализующие возможности нарушителей
1	2	3	4
1.1	Проведение атаки при нахождении в пределах контролируемой зоны	**неактуально**	Доступ в помещения размещения Системы (компонентов системы и средств защиты информации) обеспечивается в соответствии с установленным контрольно-пропускным режимом. Оператор Системы, а также Оператор ЦОД проводят работы по подбору и расстановке персонала. Администраторы системы защиты информации и Администраторы программно-аппаратного комплекса Системы проинформированы о порядке и правилах обеспечения безопасности информации при их обработке в Системе. Доступ в помещения, предназначенные для размещения СКЗИ, эксплуатационной документации и инсталлирующих носителей ограничивается в соответствии с реализованным на объектах внутриобъектовым режимом. На время проведения работ с компонентами Системы, включая компоненты СЗИ, работниками ЦОД обеспечивается временная контролируемая
1.2	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: – документацию на СКЗИ и компоненты СФ; – помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.	**неактуально**	
1.3	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:	**неактуально**	

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Факторы, нейтрализующие возможности нарушителей
1	2	3	4
	– сведений о физических мерах объектов, в которых размещены ресурсы ОП; – сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ОП; – сведений о мерах по разграничению доступа в помещения, в которых реализованы СКЗИ и СФ.		зона в помещениях проведения таких работ. Представители технических, обслуживающих и других вспомогательных служб, а также работники, не являющиеся допущенными к работе с компонентами ИТИ ЦОД, могут находиться в серверных помещениях ЦОД исключительно в присутствии уполномоченных представителей Оператора ЦОД, по согласованию с руководством. Все помещения ЦОД оснащены входными дверьми с электронными / механическими замками, также обеспечено постоянное закрытия дверей помещений и их открытие только для санкционированного прохода. Утверждены правила доступа в помещения ЦОД, где располагаются СКЗИ (могут располагаться), в рабочее и нерабочее время, а также в нештатных ситуациях. В составе Системы, а также в составе информационно-телекоммуникационной инфраструктуры ЦОД (в соответствии с зонами ответственности Операторов) используются сертифицированные средства антивирусной защиты.
1.4	Использование штатных средств Системе, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	**неактуально**	
2.1	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ	**неактуально**	
2.2	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий	**неактуально**	
3.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО	**не актуально**	В дополнение к нейтрализующим факторам, приведенным выше и обусловленным структурно-функциональными характеристиками Системы, размещением СКЗИ, реализацией пропускного и внутриобъектового режима, а также организационно-техническими и административными мерами по обеспечения безопасности информации и СКЗИ: – не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности; – реализация угроз безопасности информации, не может привести к значительным негативным последствиям, в том числе выражающимся в количественном (материальном) выражении, что также снижает мотивацию вероятного нарушителя к подготовке реализации рассматриваемой возможности атаки.
3.2	Проведение лабораторных исследований СКЗИ, используемых	**не актуально**	Аналогично п.п. 3.1 настоящей Таблицы

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Факторы, нейтрализующие возможности нарушителей
1	2	3	4
	вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий		
3.3	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ	**не актуально**	Аналогично п.п. 3.1 настоящей Таблицы
4.1	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО	**не актуально**	В дополнение к п.п. 3.1 настоящей Таблицы: – Возможности по использованию недокументированных (недекларированных) возможностей системного ПО (угрозы 1 и 2 типа) признаны неактуальными.
4.2	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	**не актуально**	Аналогично п.п. 4.1 настоящей Таблицы
4.3	Возможность воздействовать на любые компоненты СКЗИ и СФ	**не актуально**	Аналогично п.п. 4.1 настоящей Таблицы

9.3. Заключение о необходимости использования СКЗИ

В соответствии с «Методическими рекомендациями 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» (Утв. руководством 8 Центра ФСБ России 31 марта 2015 г. №149/7/2/6-432) использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию;
- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью не криптографических методов и способов.

С учётом требований нормативных и методических ФСБ России в отношении применения СКЗИ для создания системы защиты ПДн при их обработке в Системе можно заключить, что:

- в случае использования Оператором для информационного обмена ПДн и их обработки открытых каналов связи – **применение СКЗИ обязательно**;
- фактически реализуемые Оператором организационные и технические меры защиты информационно-телекоммуникационной инфраструктуры ЦОД, а также инфраструктуры Системы в значительной степени нейтрализуют угрозы, связанные с ознакомлением неавторизованных лиц с защищаемой информации, размещаемой на машинных носителях, – применение СКЗИ в целях шифрования хранящейся на них защищаемой информации не обязательно.

С учётом сведений, приведённых в Таблицах 14 – 15, определённых необходимых уровней защищённости ПДн при их обработке в Системе, а также того, что для Системы признаны актуальными угрозы 3 типа, в соответствии с Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», можно сделать вывод о необходимости применения **СКЗИ, имеющих действующий сертификат ФСБ России по классу не ниже класса КС2**, реализующих криптографические методы защиты информации для локализации каналов атак и угроз информационной безопасности, возникающих в ходе информационного взаимодействия между Системой и внутренними пользователями, осуществляющими доступ из-за пределов КЗ ЦОД. **Шифрование, как средство обеспечения конфиденциальности информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны.**

10. ЗАКЛЮЧЕНИЕ

По результатам моделирования угроз безопасности информации при её обработке в Системе, приведённых в Разделах 3 – 8 настоящей Модели угроз были выявлены актуальные угрозы безопасности информации.

Перечень актуальных угроз безопасности информации при её обработке в Системе приведён в таблице ниже (Таблица 15).

Таблица *15*. Перечень актуальных угроз безопасности информации объекта информатизации.

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).
1	2
УБИ.006	Угроза внедрения кода или данных
УБИ.010	Угроза выхода процесса за пределы виртуальной машины
УБИ.017	Угроза доступа/перехвата/ изменения HTTP cookies
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.063	Угроза некорректного использования функционала программного обеспечения
УБИ.068	Угроза неправомерного/ некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.127	Угроза подмены действия пользователя путём обмана
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.165	Угроза включения в проект недостоверно испытанных компонентов
УБИ.175	Угроза «фишинга»

Перечень актуальных угроз безопасности средств криптографической защиты информации и среды функционирования средств криптографической защиты информации приведён в таблице ниже.

Таблица *16*. Перечень актуальных угроз безопасности средств криптографической защиты информации и среды функционирования средств криптографической защиты информации.

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).
1	2
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.019	Угроза заражения DNS-кеша
УБИ.021	Угроза злоупотребления доверием потребителей облачных услуг

Идентификатор угрозы	Наименование угрозы (bdu.fstec.ru).
1	2
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
УБИ.030	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.043	Угроза нарушения доступности облачного сервера
УБИ.052	Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.064	Угроза некорректной реализации политики лицензирования в облаке
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.075	Угроза несанкционированного доступа к виртуальным каналам передачи
УБИ.077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
УБИ.078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
УБИ.096	Угроза несогласованности политик безопасности элементов облачной инфраструктуры
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.101	Угроза общедоступности облачной инфраструктуры
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.122	Угроза повышения привилегий
УБИ.127	Угроза подмены действия пользователя путём обмана
УБИ.128	Угроза подмены доверенного пользователя
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.132	Угроза получения предварительной информации об объекте защиты
УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.142	Угроза приостановки оказания облачных услуг вследствие технических сбоев
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/ передачи информации
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.164	Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.176	Угроза нарушения технологического/ производственного процесса из-за временны́х задержек, вносимых средством защиты

В соответствии с документом «Модель угроз и нарушителей безопасности персональных данных при их обработке в Облаке ИИИ (выписка)», Утвержденным Приказом Генерального директора ЗАО «ИИИ» от «03» ноября 2033 г. №000/ПДн, в отношении Облака ИИИ актуальные угрозы безопасности информации не выявлены.

Полученные характеристики угроз безопасности информации могут быть использованы для обоснования выбора средств и механизмов защиты информации Системы.

Модель угроз безопасности информации Системы должна быть пересмотрена в следующих случаях:

– внесения изменений в структурно-функциональные характеристики Системы, которые могут повлиять на защищённость обрабатываемой с её использованием информации;

– изменения перечень актуальных угроз безопасности информации центра обработки данных (облачной инфраструктуры Облака ИИИ);

– изменения технологического процесса обработки информации в Системе;

– выявления существенных недостатков по итогам контроля выполнения требований по обеспечению безопасности информации при её обработке в Системе;

– расширения (изменения) перечня угроз безопасности информации представленного в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Приложение № 1.
К Модели угроз безопасности информации
Системы

ПЕРЕЧЕНЬ ТАКТИК И СООТВЕТСТВУЮЩИХ ИМ ТЕХНИК, ПРИМЕНЕНИЕ КОТОРЫХ ВОЗМОЖНО ДЛЯ ИСПОЛЬЗОВАНИЯ СПОСОБОВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ СИСТЕМЫ

	Основные техники реализации угроз
1	**2**
Т1 Сбор информации о системах и сетях	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
	Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
	Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
	Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений
	Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств
	Т1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора.
	Т1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
	Т1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
	Т1.9 . Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей .
	Т1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
	Т1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
	Т1.13 . Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
	Т1.14 . Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
	Т1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированных паролей и ключей на специализированных

	Основные техники реализации угроз
1	**2**
	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 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
	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
Т2 Получение первоначального доступа к компонентам систем и сетей	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
	Т2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.
	Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке.
	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
	Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
	Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
	Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций.
	Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
	Т2.9. Несанкционированное подключение внешних устройств
	Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя
	Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
	Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа.
	Т2.13. Реализация атаки типа «человек посередине» для осуществления доступа.
Т3 Внедрение и исполнение вредоносного программного обеспечения в системах и сетях	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
	Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей

	Основные техники реализации угроз
1	2
	Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
	Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
	Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
	Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
	Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.
	Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.
	Т3.9. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.
	Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах
	Т3.11. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
	Т3.12. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
	Т3.13. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
	Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
	Т3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
	Т3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL
Т4 Закрепление (сохранение доступа) в системе или сети	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных
	Т4.2. Использование штатных средств удаленного доступа и управления операционной системы
	Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего

	Основные техники реализации угроз
1	**2**
	становится возможен многократный запуск вредоносного кода
	Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
	Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети
	Т4.7. 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
Т5 Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ	Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования
	Т5.2. Использование штатных средств удаленного доступа и управления операционной системы
	Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
	Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
	Т5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
	Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения
	Т5.7. Туннелирование трафика управления через VPN
	Т5.8. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
	Т5.9. Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
	Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
	Т5.11. Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
	Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.
	Т5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения
Т6 Повышение привилегий по доступу к компонентам систем и сетей	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
	Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
	Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий.

	Основные техники реализации угроз
1	2
	Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи)
	Т6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций.
	Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима
	Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с повышенными привилегиями
	Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей
	Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды.
Т7 Сокрытие действий и применяемых при этом средств от обнаружения до	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения
	Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
	Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
	Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
	Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
	Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности
	Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
	Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки
	Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей.
	Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
	Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе
	Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности

	Основные техники реализации угроз
1	2
	Т7.13. Создание скрытых файлов, скрытых учетных записей
	Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
	Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
	Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки
	Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети
	Т7.19. Туннелирование трафика управления через VPN
	Т7.20. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
	Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
	Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
	Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе
	Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи. Примечание 13: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО
	Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.
	Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах.
	Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «даркнет») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
Т8 Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
	Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
	Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования
	Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям
	Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами

	Основные техники реализации угроз
1	**2**
	Т8.6. Копирование вредоносного кода на съемные носители
	Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
	Т8.6. Копирование вредоносного кода на съемные носители
	Т8.8. Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других системах и сетях.
Т9 Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования.
	Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
	Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
	Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
	Т9.5. Отправка данных по известным протоколам управления и передачи данных
	Т9.6. Отправка данных по собственным протоколам
	Т9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения.
	Т9.8. Туннелирование трафика передачи данных через VPN
	Т9.9. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
	Т9.10. Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
	Т9.11. Отправка данных через альтернативную среду передачи данных.
	Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации
	Т9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
Т10 Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
	Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
	Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения
	Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
	Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа системного программного обеспечения
	Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства

	Основные техники реализации угроз
1	2
	T10.7. Подмена информации в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
	T10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
	T10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
	T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
	T10.11. Нецелевое использование ресурсов системы
	T10.14. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм	Номера листов (страниц)				Всего листов (страниц) в док.	№ разреш. документа	Подпись	Дата	Прим-е
	Изменен-ных	Заменен-ных	Новых	Аннулир ованных					
1	2	3	4	5	6	7	8	9	10