УТВЕРЖДАЮ
Директор МБУ ДО «ДШИ»
_____И.Э.Иванова
Приказ № 38-ОД от 01 декабря 2021 г.
М.П.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ПРИ ЕЕ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОПАЛЬНЫХ ДАННЫХ«АРМ АСУ СО ТО»

МБУ ДО «ДШИ»

ГОРОДА ВЫШНИЙ ВОЛОЧЕК

Вышний Волочек

2021 год

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящий документ предназначен для обоснования выдвигаемых требований по обеспечению безопасности персональных данных иинформации, не составляющей государственную тайну, содержащейся в автоматизированном рабочем месте пользователяАвтоматизированной системы управления системой образования Тверской области (далее – АРМ АСУ СО ТО) *МБУ ДО «ДШИ»* ,и служит основой для проведения мероприятий по созданию системы защиты информации (далее – СЗИ) АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

В ходе данной работы для АРМ АСУ СО ТО пользователябыли определены:

1. Характерные параметры угроз:

- источники угроз;
- перечень характерных сценариев реализации угроз безопасности информации и персональных данных (далее – ПДн);
- объекты воздействия угроз;
- характер и степень деструктивного воздействия на информацию и персональные данные;
- вероятность реализации угроз.

2. Возможности нарушителей, позволяющие определить класс шифровальных (криптографических) средств (далее – криптосредств), предполагаемых для использования в АРМ АСУ СО ТО, в соответствии с документами:

- Приказ ФСБ России от 10июля 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».

Актуальность реализации угроз безопасности информации и персональных данных для АРМ АСУ СО ТО определялась в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержденной заместителем директора ФСТЭК России 14 февраля 2008 г.).

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Доступность – свойство информации при ее обработке техническими средствами, обеспечивающее беспрепятственный доступ к ней для проведения санкционированных операций по ознакомлению, документированию, модификации и уничтожению.

Защита информации от НСД– деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации (ГОСТ Р 50922 – 96).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ФЗ – 152).

Контролируемая зона– это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ФЗ – 149).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ФЗ – 152).

Оператор–государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (ФЗ – 152).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (ГОСТ Р 51624 – 2000).

Уничтожение персональных данных– действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ФЗ – 152).

Уязвимость компьютерной системы – это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Целостность – свойство информации быть неизменной в условиях случайного или преднамеренного искажения (разрушения).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АИС	–	Автоматизированная информационная система
АРМ	–	Автоматизированное рабочее место
ИБ	–	Информационная безопасность
ИР	–	Информационные ресурсы
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
ИТС	–	Информационно-телекоммуникационная сеть
КЗ	–	Контролируемая зона
МЭ	–	Межсетевой экран
НСД	–	Несанкционированный доступ
НДВ	–	Недекларированные возможности
ОС	–	Операционная система
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
ПЭМИН	–	Побочные электромагнитные излучения и наводки
СЗПДн	–	Система защиты персональных данных
СКЗИ	–	Средства криптографической защиты информации
СКУД	–	Система контроля и управления доступом
СМЭВ	–	Система межведомственного электронного взаимодействия
СФК	–	Среда функционирования криптосредств
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю
ЦОД	–	Центр обработки данных
BIOS	–	Basicinput/outputsystem
DNS	–	DomainNameSystem
HTTPS	–	HyperTextTransferProtocolSecure
VPN	–	VirtualPrivateNetwork
UEFI	–	UnifiedExtensibleFirmwareInterface
152-ФЗ	–	Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»
ПП 1119	–	Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 1 ноября 2012

ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ

В ходе подготовки настоящейЧастной модели угроз были использованы положения следующих нормативных документов:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.
6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1 ОПИСАНИЕАВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ПОЛЬЗОВАТЕЛЯ

1.1 Общее описание автоматизированного рабочего места пользователя

АРМ АСУ СО ТО *МБУ ДО «ДШИ»* представляет собой информационную систему, реализующую возможность доступа к АСУ СО ТО.

АРМ АСУ СО ТО *МБУ ДО «ДШИ»* размещен по адресу: 171158 Тверская область, г.В.Волочек, ул.Вагжанова, д.30, офис 316.

1.2 Пользователи системы

К пользователям АРМ АСУ СО ТО *МБУ ДО «ДШИ»* относятся:

- пользователи – сотрудники организаций, осуществляющих образовательную деятельность на территории Тверской области. Доступ таким пользователям должен предоставляться согласно требованиям документа «Технические условия для подключения объектов к АСУ СО ТО»;
- привилегированные пользователи – администраторы функциональных модулей, администратор СЗИ, разработчики прикладного ПО.

АРМ АСУ СО ТО *МБУ ДО «ДШИ»* является системой, в которой права доступа к обрабатываемой информации различны для различных групп пользователей.

1.3 Состав обрабатываемых данных

Винформационной системе АРМ АСУ СО ТО *МБУ ДО «ДШИ»* обрабатываются следующие персональные данные учеников:

- фамилия, имя, отчество;
- дата рождения;
- место рождения по ОКАТО/ОКСМ;
- пол (м/ж);
- номер СНИЛС;
- гражданство (российское/иностранное/без гражданства);
- данные свидетельства о рождении (серия и номер, дата выдачи, кем выдан);
- данные документа, удостоверяющего личность (тип документа, серия и номер, кем, где и когда выдан);
- адрес регистрации по месту жительства (полный адрес, населенный пункт по ОКАТО/ОКТМО);

- адрес регистрации по месту пребывания (полный адрес, населенный пункт по ОКАТО/ОКТМО);
- адрес фактического места жительства (полный адрес, населенный пункт по ОКАТО/ОКТМО);
- социальный статус:
    - дети, оставшиеся без попечения родителей, основания статуса (смерть родителей, лишение родительских прав и пр.);
    - дети инвалиды;
    - дет с ограниченными возможностями здоровья;
    - дет-жертвы вооруженных и межнациональных конфликтов, экологических и техногенных катастроф, стихийных бедствий;
    - дети из семей беженцев и вынужденных переселенцев;
    - дети, оказавшиеся в экстремальных условиях;
    - дети-жертвы насилия;
    - дети, отбывающие наказание в виде лишения свободы в воспитательных колониях;
    - дети, находящиеся в образовательных организациях для обучающихся с девиантным поведением, нуждающихся в особых условиях воспитания, обучения и требующих специального педагогического подхода (специальных учебно-воспитательных учреждениях открытого и закрытого типа);
    - дети, проживающие в малоимущих семьях;
    - дети с отклонениями в поведении;
    - дети, жизнедеятельность которых объективно нарушена в результате сложившихся обстоятельств и которые не могут преодолеть данные обстоятельства самостоятельно или с помощью семьи.
- группа здоровья;
- физкультурная группа;
- инвалидность (группа инвалидности, срок действия, категория (при наличии));
- данные о наличии потребности в адаптированной программе обучения:
    - вид программы;
    - наличие заключение психолого-медико-педагогической комиссии (номер заключения, дата заключения) и (или)
    - индивидуальной программы ребенка (номер заключения, дата заключения).

- данные об образовании:
    - дошкольном образовании (место получения образования, форма образования, дата начала обучения, образовательная программа, режим пребывания, дата и причина окончания обучения);
    - общем (место получения образования, форма образования, дата начала обучения, год обучения, данные об освоении программ (уровень общего образования, вид программы обучения), данные о смене, портфолио, итого ГИА/ГВЭ/ЕГЭ, дата и причина окончания обучения, данные документа об обучении (номер, дата выдачи));
    - среднем профессиональном (место получения образования, форма образования, дата начала обучения, курс обучения, данные об освоении программ (наименование, профиль (специализация), вид, статус, итоговые оценки), дата и причина окончания обучения, данные документа об обучении (реквизиты, дата выдачи));
    - дополнительном (место получения образования, дата начала обучения, год (курс) обучения, данные об освоении программ(наименование,вид, статус, итоговые оценки), дата и причина окончания обучения, данные документа об обучении (реквизиты, дата выдачи));
    - специальном (место получения образования, дата начала обучения, год (курс) обучения, специальность (профессия), данные об освоении программ (наименование, дата начала и окончания, статус, итоговые оценки), дата и причина окончания обучения, данные документа о квалификации (реквизиты, дата выдачи)).

В информационной системе АРМ АСУ СО ТО *МБУ ДО «ДШИ»* обрабатываются следующие персональные данные родителей (законных представителей) учеников:

- родство (мать, отец) или тип законного представителя (опекун/попечитель/орган опеки и попечительства/усыновитель/приемный родитель);
- фамилия, имя, отчество;
- дата рождения;
- номер СНИЛС;
- гражданство (российское/иностранное/без гражданства);
- данные документа, удостоверяющего личность (тип документа, серия и номер, дата и место выдачи);
- данные документа, удостоверяющего положение законного представителя по отношению к ребенку – при необходимости.

1.4 Взаимодействие со смежнымисистемами

АРМ АСУ СО ТО *МБУ ДО «ДШИ»* взаимодействует с АСУ СО ТО – информационной системой, размещеннойв центре обработки данных (далее – ЦОД) на территории Государственного бюджетного образовательного учреждения дополнительного профессионального образования Тверской областной институт усовершенствования учителей (далее – ГБОУ ДПО ТОИУУ), по адресу: Россия, Тверская обл., г. Тверь, Волоколамский пр-т, д. 7, кабинет 314.

Взаимодействие осуществляется средствами подключения пользователей АРМ АСУ СО ТО *МБУ ДО «ДШИ»* к АСУ СО ТО с использованием сетей общего доступа.

Общая схема взаимодействия АРМ АСУ СО ТО *МБУ ДО «ДШИ»* с АСУ СО ТО представлена на Рисунке 1.

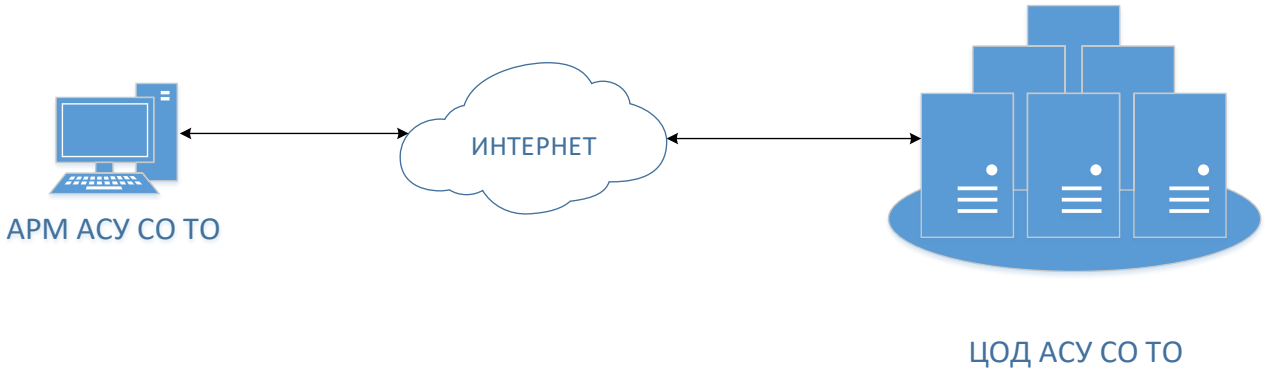

Рисунок 1 – Схема соединения с ЦОД

1.5 Компоненты

Состав комплекса технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»* и их описание представлены в Таблице 1.

Таблица 1–Комплекс технических средств АСУ СО ТО *МБУ ДО «ДШИ»*

№ п/п	Компонент	Роль	Размещение	Тип	Программная архитектура
1.	АРМ АСУ СО ТО *МБУ ДО «ДШИ»*	Персональное автоматизированное рабочее место для доступа к АСУ СО ТО	…	Физическое оборудование	…

1.6 Реализованные защитные меры

1.6.1 Организационные меры

В настоящее время приняты следующие организационные меры по обеспечению безопасности информации и персональных данных:

1. Разработан документ, определяющий политику обработки персональных данных субъектов в *МБУ ДО «ДШИ»* .
2. Разработан ряд документ, определяющий правила обработки персональных данных в *МБУ ДО «ДШИ»* , правила осуществления контроля соответствия такой обработки, правила рассмотрения и ответов на запросы субъектов ПДн.
3. Назначен ответственный за обработку ПДн в *МБУ ДО «ДШИ»* .
4. Разработан документ, определяющий порядок доступа работников *МБУ ДО «ДШИ»* в помещения, в которых ведется обработка ПДн, а также документ, определяющий перечень сотрудников, чьи должности предусматривают обработку ПДн.
5. Обеспечено получение обязательства о прекращении обработки ПДн сотрудников *МБУ ДО «ДШИ»* в случае расторжения с ним трудового договора.
6. Разработан ряд технических документов, определяющих обязанности администратора ИБ в *МБУ ДО «ДШИ»* , определяющих обязанности пользователя информационной системы, порядок обслуживания технических средств, порядок и правила проведения антивирусного контроля в информационной системе, порядок и правила применения парольной защиты в информационной системе, регламент осуществления резервного копирования и восстановления данных.

1.6.2 Технические меры

К техническим мерам относятся методы и способы защиты информации, содержащей ПДн и обрабатываемой с использованием средств вычислительной техники. Порядок технической защиты устанавливается Правительством Российской Федерации (Постановление №1119), ФСТЭК России (Приказ №21), ФСБ России (Приказ ФСБ №378).

В настоящее время в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* приняты следующие технические меры по обеспечению безопасности персональных данных:

1. Используются стандартные средства ОС для:
    a. Создания учетных записей пользователей и управления ими;
    b. Идентификации и аутентификации пользователей;
    c. Разграничения доступа по установленным правилам;
    d. Разделения ролей пользователей (администратор, пользователь);
    e. Создания парольной политики (требования к паролю, ограничение

числа неуспешных попыток входа в систему)

f. Блокирование сеанса доступа после установленного времени бездействия и по запросу пользователя;

g. Определение и регистраций событий безопасности;

2. Проводятся регулярное техническое обслуживание и замена устаревшихкомпонентов.

1.6.3 Меры и средства физической защиты

Для обеспечения физической защиты АРМ АСУ СО ТО *МБУ ДО «ДШИ»* реализованы следующие меры:

1. АРМАСУ СО ТО *МБУ ДО «ДШИ»* размещено в пределах контролируемой зоны образовательного учреждения.

2. На территории образовательного учреждения соблюдаются меры противопожарной безопасности.

3. АРМ АСУ СО ТО *МБУ ДО «ДШИ»* размещено в запираемом помещении, доступ к которому имеет ограниченный круг лиц.

2 МОДЕЛИРОВАНИЕУГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

2.1 Определение класса защищенности автоматизированного рабочего места пользователя и уровня защищенности персональных данных

Основные характеристики АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , необходимые для построения модели угроз, приведены в Таблице 2.

Таблица2 – Основные характеристики АРМ АСУ СО ТО *МБУ ДО «ДШИ»*

Наименование характеристики	Значение
Категория обрабатываемых персональных данных	Иные, специальные
Обрабатываемые ПДн	ПДн субъектов, не являющихся сотрудниками оператора
Объем обрабатываемых персональных данных	Менее 100 000
Структура информационной системы	Локальная
Наличие подключения к сетям связи общего пользования и/или сетям международного информационного обмена	Имеет
Режим обработки персональных данных	Многопользовательский
Наличие разграничения доступа	С разграничением прав доступа
Местонахождение технических средств информационной системы	Все средства находятся в пределах РФ

Типы угроз, актуальные для АРМ АСУ СО ТО,приведены в Таблице 3.

Таблица 3–Актуальные типы угроз

Тип угрозы	Актуальность	Примечание
1 тип	Не актуально	Угрозы, связанные с наличием НДВ в системном и прикладном ПО, признаются неактуальными в связи с: – использованием лицензионного, постоянно обновляемого системного и прикладного ПО известных мировых и российских производителей; – заключением договоров на разработку и/или модернизацию используемого прикладного ПО, содержащих четкие требования к его функциональности, предусматривающих
2 тип		

Тип угрозы	Актуальность	Примечание
		ответственность разработчика за несоблюдение условий договора; – заключением соглашений о конфиденциальности с разработчиками, предусматривающих ответственность за несанкционированное разглашение конфиденциальной информации; – превышением стоимости защиты от данных типов угроз стоимости защищаемой информации.
3 тип	Актуально	Угрозы, не связанные с НДВ прикладного и системного ПО.

В соответствии с Актом определения уровня защищенности персональных данных при их обработке в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , при построении системы защиты АРМ АСУ СО ТО *МБУ ДО «ДШИ»* необходимо обеспечить **третий уровень защищенности** персональных данных.

2.2 Определение исходной защищенностиавтоматизированного рабочего места пользователя

Под уровнем исходной защищенности АРМ АСУ СО ТО *МБУ ДО «ДШИ»* понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик АРМ АСУ СО ТО *МБУ ДО «ДШИ»* . Результаты определения уровня исходной защищенности АРМ АСУ СО ТО *МБУ ДО «ДШИ»* представлены в Таблице 4.

Таблица4 – Показатели исходной защищенности АРМ АСУ СО ТО *МБУ ДО «ДШИ»*

Технические и эксплуатационные характеристики	Уровень защищенности	Пояснение
По территориальному размещению	Высокий	Локальная ИСПДн, развернутая в пределах одного здания
По наличию соединения с сетями общего пользования	Средний	ИСПДн, имеющая одноточечный выход в сеть общего пользования
По встроенным (легальным) операциям с записями баз персональных данных	Высокий	Чтение, поиск

Технические и эксплуатационные характеристики	Уровень защищенности	Пояснение
По разграничению доступа к персональным данным	Средний	ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцемИСПДн, либо субъект ПДн;
По наличию соединений с другими базами ПДн иных ИСПДн	Высокий	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн
По уровню обобщения (обезличивания) ПДн	Низкий	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными
По объему ПДн, предоставляемых сторонним пользователям ИСПДн без предварительной обработки	Высокий	ИСПДн, предоставляющая часть ПДн

Итого ответов: высокий – 4 (57%), средний –2 (29%), низкий – 1 (14%).

Таким образом, исходный уровень защищенности АРМ АСУ СО ТО *МБУ ДО «ДШИ»* следует оценивать, как **средний**. В расчетах актуальности угроз следует применять коэффициент исходной защищенности $\mathbf{Y_1 = 5}$.

2.3 Определение возможных каналов доступа к ресурсам автоматизированного рабочего места пользователя

При попытке несанкционированного доступа к защищаемым ресурсам АРМ АСУ СО ТО *МБУ ДО «ДШИ»* (попытке атаки) нарушитель в общем случае может использовать следующие каналы:

- канал непосредственного доступа к объекту атаки (физический);
- общедоступные каналы связи, по которым осуществляется передача информации ограниченного доступа;
- технические каналы утечки информации (видовой, ПЭМИН, акустический).

С учетом введенных организационно-технических мер по ограничению доступа в помещения, в которых размещается АРМАСУ СО ТО *МБУ ДО «ДШИ»* , реализация угроз безопасности информации, связанных с перехватом ПЭМИН в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , нереализуема, так как технические средства АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , создающие физические поля, находятся в пределах контролируемой зоны, поэтому **угрозы утечки информации по каналам ПЭМИН являются неактуальными.**

В АРМ АСУ СО ТО *МБУ ДО «ДШИ»* не предусмотрены голосовой ввод и воспроизведение информации, содержащей персональные данные, а также ее обсуждение в процессе обработки, в связи с чем**угрозы утечки информации по акустическому каналу являются неактуальными**.

2.4 Определение источников угроз (модель нарушителя безопасности информации)

Источниками угроз являются нарушители режима информационной безопасности АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , т.е. лица (или инициируемые ими процессы), неумышленно нарушающие свойства безопасности информации, либо проводящие атаку на АРМАСУ СО ТО *МБУ ДО «ДШИ»* .

Виды нарушителей по отношению к АРМ АСУ СО ТО *МБУ ДО «ДШИ»* подразделяются на:

- внутренних нарушителей, имеющих доступ к АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , включая пользователей АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , реализующих угрозы в контролируемой зоне;
- внешних нарушителей, не имеющих доступа к АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , реализующих угрозы из-за пределов контролируемой зоны.

Основными нарушителями безопасности информации в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* являются:

- внешний нарушитель (криминальные структуры, внешние субъекты – физические лица) – N1;
- лица, не являющиеся зарегистрированными пользователями и не допущенные к работе в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , но имеющие санкционированный доступ в КЗ – N2;
- зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , осуществляющие доступ к информационной системе и/или части данных – N3;
- зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* с полномочиями системного администратора– N4;

- зарегистрированные пользователи с полномочиями администратора ИБ АРМ АСУ СО ТО *МБУ ДО «ДШИ»* – N5;
- разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»* – N6.

Детальное описание модели нарушителя АРМ АСУ СО ТО *МБУ ДО «ДШИ»* представлено в Приложении А настоящего документа.

В настоящей модели не рассматриваются в качестве актуальных нарушители **N2,N3,N4,N5, N6**, к которым относятся следующие категории пользователей:

- обслуживающий персонал, не имеющий доступа к информации: сотрудники *МБУ ДО «ДШИ»* , сотрудники обслуживающих организаций, имеющих доступ на территорию и т.п;
- зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , осуществляющие обработку информации;
- системные администраторы АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- администратор ИБ АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

Предполагается, что лица, имеющие доступ в контролируемую зону, но не являющиеся пользователями ИСПДн АРМ АСУ СО ТО *МБУ ДО «ДШИ»* – обслуживающий персонал, назначается из числа доверенных лиц.Их доверенность обеспечивается комплексом реализованных режимных, организационных, кадровых мер по подбору персонала и контролю их лояльности и трудов деятельности.

Предполагается, что сотрудники, являющиеся зарегистрированными пользователям АСУ СО ТО *МБУ ДО «ДШИ»* , и обладающие легальным доступом к обрабатываемой информации, проходят соответствующую подготовку и инструктаж по особенностям обработки информации в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* и основам информационной безопасности. Для контроля действия таких пользователей применяются штатные средства ОС для регистрации и отслеживания событий, позволяющие осуществлять контроль и анализ действий пользователей.

Предполагается, что сотрудники, наделенные полномочиями администраторов АСУ СО ТО *МБУ ДО «ДШИ»* , назначаются из числа доверенных сотрудников. Их доверенность обеспечивается комплексом реализованных режимных, организационных, кадровых мер по подбору персонала и контролю их лояльности и трудов деятельности. Также предполагается, что разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АСУ СО ТО *МБУ ДО «ДШИ»* , являются доверенными. Их доверенность

обеспечивается комплексом организационных мер (использованием лицензионного, постоянно обновляемого системного и прикладного ПО известных мировых и российских производителей; заключением договоров на разработку и/или модернизацию используемого прикладного ПО, содержащих четкие требования к его функциональности, предусматривающих ответственность разработчика за несоблюдение условий договора; заключением соглашений о конфиденциальности с разработчиками, предусматривающих ответственность за несанкционированное разглашение конфиденциальной информации).

Также предполагается, что потенциальные нарушители являются одиночными нарушителями, самостоятельно осуществляющими освоение способов, подготовку и проведение атак и не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, в том числе специализирующихся в области разработки и анализа СКЗИ и СФК.

В качестве **актуальных нарушителей** в данной модели рассматриваются нарушители **N1**:

– внешние субъекты – физические лица;

Согласно Приказу ФСБ №378, для обеспечения **3 уровня защищенности** персональных данных при их обработке в информационной системе и актуальных угрозах 3 типа, должны применяться СКЗИ класса КС1 и выше. Исходя из результатов анализа способов получения исходных данных при создании способов, подготовке и проведении атак злоумышленников (см. Приложение А настоящего документа), для обеспечения безопасности персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее – атака), должны применяться **СКЗИ класса не ниже КС1**.

2.5 Расчет параметров для угроз и определение их актуальности

2.5.1 Расчет вероятности реализации угроз безопасности информации

Под вероятностью реализации угрозы (Y_2) понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной АРМ АСУ СО ТО *МБУ ДО «ДШИ»* в складывающихся условиях обстановки.

Вводятся четыре вербальных градации этого показателя:

– Y_2 = 0 – маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации

лицами, не имеющими легального доступа в помещение, где хранятся носители информации);

- Y_2 = 2 – низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (в организации внедрены средства защиты от данной угрозы и приняты организационные меры по минимизации возможности ее реализации);
- Y_2 = 5 – средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности информации недостаточны (в организации не внедрены средства защиты от данной угрозы или не приняты организационные меры по минимизации возможности ее реализации);
- Y_2 = 10 – высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности информации не приняты (в организации не внедрены средства защиты от данной угрозы и не приняты организационные меры по минимизации возможности ее реализации).

Значение данного параметра вносится в столбец «Вероятность» таблиц Приложения Б для каждой из рассматриваемых угроз.

2.5.2 Оценка размера последствий для субъекта ПДн от реализации каждой угрозы безопасности ПДн (опасности угроз)

Опасность угроз напрямую определяется теми последствиями для субъекта ПДн, к которым приводит их реализация. Последствия для субъекта ПДн определяются в виде показателя опасности угрозы. Критерии для определения размера последствий для субъекта ПДн и соответствующих показателей опасности угрозы определяются на основе опроса экспертов (специалистов в области защиты информации).

Экспертные оценки уровня ущерба для субъектов ПДн от воздействия угроз, полученные в ходе проведения обследования информационных систем, приведены в Таблице 5.

Таблица 5 – Показатели опасности угроз в АСУ СО ТО *МБУ ДО «ДШИ»*

Наименование характеристики безопасности ПДн	Размер последствий для субъекта ПДн	Показатель опасность угрозы*
Конфиденциальность	Негативные последствия для субъектов персональных данных	Средняя
Целостность	Негативные последствия для субъектов персональных данных	Средняя
Доступность	Негативные последствия для субъектов персональных данных	Средняя

*– является экспертной оценкой.

Значение данного параметра вносится в столбец «Опасность» таблиц Приложения Б для каждой из рассматриваемых угроз.

2.5.3 Определение актуальных угроз из полученного общего перечня угроз безопасностиинформации, характерных для анализируемой АСУ СО ТО *МБУ ДО «ДШИ»*

На данном этапе проводится экспертная оценка сформированных наборов угроз безопасности информации с точки зрения частоты (вероятности) их реализации с определением для каждой угрозы соответствующего числового коэффициента (Y_2), и производится вычисление коэффициентов реализуемости выявленных угроз (Y) в соответствии с формулой:

$$Y = \frac{(Y1 + Y2)}{20}$$

с последующей вербальной интерпретацией полученных коэффициентов для всех выявленных угроз в диапазоне «низкая – средняя – высокая – очень высокая».

По итогам вычислений коэффициента реализуемости угрозы Y для каждой угрозы формируется вербальная интерпретация реализуемости угрозы следующим образом:

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

Далее определяется актуальность каждой из угроз безопасности информации для АСУ СО ТО *МБУ ДО «ДШИ»* , в соответствии с Таблицей 6.

Таблица6 – Параметры определения актуальности угроз безопасности информации

Возможностьреализации угрозы(*Y*)	Показатель опасности угрозы		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Значение данного параметра вносится в столбец «Актуальность» таблиц Приложения Б для каждой из рассматриваемых угроз.

2.6 Актуальные угрозы безопасности информации, обрабатываемойна автоматизированном рабочем месте

Перечень актуальных угроз безопасности информации, обрабатываемой в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , составленный по результатам проведенного моделирования, приведен в Таблице 7. Детальное описание возможных источников угроз (Модели нарушителя) представлено в Приложении А настоящего документа. Результаты моделирования и оценки актуальности угроз безопасности информации представлены в Приложении Б настоящего документа.

Таблица 7–Актуальные угрозы

ID	Название угрозы
У.6	Угроза внедрения кода или данных
У.8	Угроза восстановления аутентификационной информации
У.14	Угроза длительного удержания вычислительных ресурсов пользователями
У.15	Угроза доступа к защищаемым файлам с использованием обходного пути
У.16	Угроза доступа к локальным файлам сервера при помощи URL
У.17	Угроза доступа/перехвата/изменения HTTP cookies
У.19	Угроза заражения DNS-кеша
У.22	Угроза избыточного выделения оперативной памяти
У.28	Угроза использования альтернативных путей доступа к ресурсам
У.30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию

ID	Название угрозы
У.31	Угроза использования механизмов авторизации для повышения привилегий
У.34	Угроза использования слабостей протоколов сетевого/локального обмена данными
У.41	Угроза межсайтового скриптинга
У.42	Угроза межсайтовой подделки запроса
У.49	Угроза нарушения целостности данных кеша
У.62	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
У.69	Угроза неправомерных действий в каналах связи
У.71	Угроза несанкционированного восстановления удалённой защищаемой информации
У.74	Угроза несанкционированного доступа к аутентификационной информации
У.83	Угроза несанкционированного доступа к системе по беспроводным каналам
У.86	Угроза несанкционированного изменения аутентификационной информации
У.88	Угроза несанкционированного копирования защищаемой информации
У.89	Угроза несанкционированного редактирования реестра
У.90	Угроза несанкционированного создания учётной записи пользователя
У.91	Угроза несанкционированного удаления защищаемой информации
У.93	Угроза несанкционированного управления буфером
У.98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
У.100	Угроза обхода некорректно настроенных механизмов аутентификации
У.103	Угроза определения типов объектов защиты
У.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
У.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
У.116	Угроза перехвата данных, передаваемых по вычислительной сети
У.121	Угроза повреждения системного реестра
У.122	Угроза повышения привилегий
У.124	Угроза подделки записей журнала регистрации событий
У.128	Угроза подмены доверенного пользователя

ID	Название угрозы
У.130	Угроза подмены содержимого сетевых ресурсов
У.139	Угроза преодоления физической защиты
У.140	Угроза приведения системы в состояние «отказ в обслуживании»
У.145	Угроза пропуска проверки целостности программного обеспечения
У.152	Угроза удаления аутентификационной информации
У.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
У.155	Угроза утраты вычислительных ресурсов
У.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
У.158	Угроза форматирования носителей информации
У.159	Угроза «форсированного веб-браузинга»
У.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
У.162	Угроза эксплуатации цифровой подписи программного кода
У.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
У.170	Угроза неправомерного шифрования информации
У.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
У.172	Угроза распространения «почтовых червей»
У.174	Угроза «фарминга»
У.175	Угроза «фишинга»
У.176	Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
У.178	Угроза несанкционированного использования системных и сетевых утилит
У.179	Угроза несанкционированной модификации защищаемой информации
У.180	Угроза отказа подсистемы обеспечения температурного режима
У.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
У.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
У.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
У.192	Угроза использования уязвимых версий программного обеспечения
У.197	Угроза хищения аутентификационной информации из временных файлов cookie

ID	Название угрозы
У.198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
У.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
У.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты

ЗАКЛЮЧЕНИЕ

В настоящем документе определены актуальные угрозы, воздействующие на АРМ АСУ СО ТО *МБУ ДО «ДШИ»* . Сведения, приведенные в документе,являются основой для проектирования системы защиты информации, обрабатываемой в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

Для построения системы защиты АРМ АСУ СО ТО *МБУ ДО «ДШИ»* требуется провести следующие мероприятия:

1. Внедрить комплексное средство защиты информации, реализующее функции защиты информации от несанкционированного доступа, антивирусной защиты, межсетевого экранирования и обнаружения вторжений на уровне хоста.
2. Обеспечить криптографическую защиту каналов связи между АРМ АСУ СО ТО *МБУ ДО «ДШИ»* и АСУ СО ТО (в соответствии с требованиями Приказа ФСБ России № 378).
3. Реализовать требования регламента взаимодействия со смежными информационными системами или иного документа, описывающего требования по защите информации при подключении АРМ АСУ СО ТО *МБУ ДО «ДШИ»* к АСУ СО ТО.

ПРИЛОЖЕНИЕ А. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ

Источниками угроз являются нарушители режима информационной безопасности в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , т.е. лица (или инициируемый ими процесс), неумышленно нарушающие свойства безопасности информации, либо проводящие атаку на объекты воздействия АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

Виды нарушителей в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* подразделяются на (см. ТаблицуА.1):

- внутренних нарушителей, имеющих доступ в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , включая пользователей АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , реализующих угрозы из контролируемо зоны;
- внешних нарушителей, не имеющих доступа к АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , реализующих угрозы из-за пределов контролируемой зоны.

Основными нарушителями безопасности информации в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* являются:

- внешний нарушитель (конкуренты, криминальные структуры, внешние субъекты – физические лица);
- лица, не являющиеся зарегистрированными пользователями и не допущенные к АРМАСУ СО ТО *МБУ ДО «ДШИ»* , но имеющие санкционированный доступ в КЗ;
- зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , осуществляющие доступ к информационной системе;
- зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* с правами системного администратора;
- зарегистрированные пользователи с полномочиями администратора ИБ АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

ТаблицаА.1–Соответствие типов и категорий нарушителей организационно-штатной структуре

Тип нарушителя	Категории нарушителей	Категории пользователей	Потенциал нарушителя	Иден-р ФСТЭК
Внешний нарушитель	Внешний нарушитель (криминальные структуры, внешние субъекты – физические лица)	-	Низкий	N1
Внутренний нарушитель	Лица, не являющиесязарегистрированными пользователями и не допущенные к работе вАРМ АСУ СО ТО *МБУ ДО «ДШИ»* , ноимеющие санкционированный доступ в КЗ	Обслуживающий персонал, не имеющий доступа к ПДн: – сотрудники обслуживающих организаций, имеющих доступ на территорию и т.п.	Низкий	N2
	Зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , осуществляющие доступ к сегменту информационной системе	Пользователи веб-сервисов информационной системы – сотрудники организации	Низкий	N3
	Зарегистрированные пользователи АРМ АСУ СО ТО *МБУ ДО «ДШИ»* с полномочиями системного администратора	Сотрудники организации	Средний	N4
	Зарегистрированные пользователи с полномочиями администратора ИБ АРМ АСУ СО ТО *МБУ ДО «ДШИ»*	Администратор ИБ АРМ АСУ СО ТО *МБУ ДО «ДШИ»*	Высокий	N5
	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»*	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»*	Высокий	N6

Возможности нарушителя N1:

- могутосуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- могутосуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- могутосуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ;
- могутосуществлять несанкционированный доступ через элементы информационной инфраструктуры АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

Возможности нарушителя N2:

- могут располагать фрагментами информации об используемых коммуникационных протоколах и их сервисах;
- могут иметь информацию о работниках организации, являющихся пользователями или администраторами АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- могут иметь информацию о местах хранения конфиденциальной информации;
- могут иметь информацию об атрибутах, обеспечивающих доступ к некоторому подмножеству ресурсов, не содержащих ПДн;
- могут иметь информацию о ресурсах АРМ АСУ СО ТО *МБУ ДО «ДШИ»* : порядок и правила создания, хранения и передачи информации, форматы сообщений, структура и свойства информационных потоков.

Возможности нарушителя N3:

- могут иметь информацию об атрибутах, обеспечивающих доступ к некоторому подмножеству ресурсов, содержащих ПДн;
- могут иметь информацию о структуре, функциях, принципах, механизмах действия и правилах работы технических средств и средств защиты информации в объеме эксплуатационной документации;
- могут иметь информацию о функциональных особенностях АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;

- могут иметь информацию о ресурсах АРМ АСУ СО ТО *МБУ ДО «ДШИ»* : порядок и правила создания, хранения и передачи информации, форматы сообщений, структура и свойства информационных потоков;
- могут иметь информацию о некоторых уязвимостях АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- могут обладать сведениями о возможных для АРМ АСУ СО ТО *МБУ ДО «ДШИ»* каналах атак;

Возможности нарушителя N4:

- могут иметь информацию об атрибутах, обеспечивающих доступ к некоторому подмножеству ресурсов, содержащих ПДн;
- могут иметь информацию о структуре, функциях, принципах, механизмах действия и правилах работы технических средств и средств защиты информации в объеме эксплуатационной документации;
- могут иметь информацию о функциональных особенностяхАРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- могут иметь информацию о ресурсах АРМ АСУ СО ТО *МБУ ДО «ДШИ»* : порядок и правила создания, хранения и передачи информации, форматы сообщений, структура и свойства информационных потоков;
- могут иметь информацию о некоторыхуязвимостях АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- могут обладать сведениями о возможных для АРМ АСУ СО ТО *МБУ ДО «ДШИ»* каналах атак.
- располагают именами и могут вести выявление паролей зарегистрированных пользователей АРМ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- обладают правами конфигурирования и административной настройки АРМ АСУ СО ТО *МБУ ДО «ДШИ»* .

Возможности нарушителя N5:

- обладают полной информацией об АСУ СО ТО *МБУ ДО «ДШИ»* ;
- имеют доступ к информации, содержащей ПДн и распространяющейся по внутренним каналам связи АСУ СО ТО *МБУ ДО «ДШИ»* ;
- обладают полной информацией о системном и прикладном программном обеспечении, используемом в АСУ СО ТО *МБУ ДО «ДШИ»* ;
- обладают полной информацией о технических средствах и конфигурации АСУ СО ТО *МБУ ДО «ДШИ»* ;

- располагают именами и могут вести выявление паролей зарегистрированных пользователей;
- имеют доступ ко всем техническим средствам обработки информации и даннымАСУ СО ТО *МБУ ДО «ДШИ»* ;
- обладают правами конфигурирования и административной настройки технических средствАСУ СО ТО *МБУ ДО «ДШИ»* .

Возможности нарушителя N6:

- обладают информацией об используемых технических средствах, а также алгоритмах их работы и недекларированных возможностях;
- обладают возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения.

В настоящей модели не рассматриваются в качестве актуальных нарушители **N2,N3,N4,N5, N6**, к которым относятся следующие категории пользователей:

- обслуживающий персонал, не имеющий доступа к информации: сотрудники *МБУ ДО «ДШИ»* , сотрудники обслуживающих организаций, имеющих доступ на территорию и т.п;
- зарегистрированные пользователи АСУ СО ТО *МБУ ДО «ДШИ»* , осуществляющие обработку информации;
- системные администраторы АСУ СО ТО *МБУ ДО «ДШИ»* ;
- администратор ИБ АСУ СО ТО *МБУ ДО «ДШИ»* ;
- разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АСУ СО ТО *МБУ ДО «ДШИ»* .

Предполагается, что лица, имеющие доступ в контролируемую зону, но не являющиеся пользователями ИСПДн АРМ АСУ СО ТО *МБУ ДО «ДШИ»* – обслуживающий персонал,назначается из числа доверенных лиц.Их доверенность обеспечивается комплексом реализованных режимных, организационных, кадровых мер по подбору персонала и контролю их лояльности и трудов деятельности.

Предполагается, что сотрудники, являющиеся зарегистрированными пользователям АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , и обладающие легальным доступом к обрабатываемой информации, проходят соответствующую подготовку и инструктаж по особенностям обработки информации в АРМ АСУ СО ТО *МБУ ДО «ДШИ»* и основам информационной безопасности. Для контроля действия таких пользователей применяются средства регистрации и учета событий информационной безопасности, позволяющие осуществлять контроль и анализ действий пользователей.

Предполагается, что сотрудники, наделенные полномочиями администраторовАРМ АСУ СО ТО *МБУ ДО «ДШИ»* , назначаются из числа доверенных сотрудников. Их доверенность обеспечивается комплексом реализованных режимных, организационных, кадровых мер по подбору персонала и контролю их лояльности и трудов деятельности.Также предполагается, что разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АРМ АСУ СО ТО *МБУ ДО «ДШИ»* , являются доверенными. Их доверенность обеспечивается комплексом организационных мер (использованием лицензионного, постоянно обновляемого системного и прикладного ПО известных мировых и российских производителей; заключением договоров на разработку и/или модернизацию используемого прикладного ПО, содержащих четкие требования к его функциональности, предусматривающих ответственность разработчика за несоблюдение условий договора; заключением соглашений о конфиденциальности с разработчиками, предусматривающих ответственность за несанкционированное разглашение конфиденциальной информации).

Также предполагается, что потенциальные нарушители являются одиночными нарушителями, самостоятельно осуществляющими освоение способов, подготовку и проведение атак, и не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, в том числе специализирующихся в области разработки и анализа СКЗИ и СФК.

В качестве **актуальных нарушителей** в данной модели рассматриваются нарушители **N1**:

– криминальные структуры, внешние субъекты – физические лица.

Исходя из полученных на этапе обследования АРМ АСУ СО ТО *МБУ ДО «ДШИ»* сведений, злоумышленником могут быть использованы следующие способы получения исходных данных при создании способов, подготовке и проведении атак, представленные в Таблице А.2.

Таблица А.2–Способы получения исходных данных

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	**+/—**	**Пояснение**
СКЗИ класса КС1		
а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;	+	Согласно построенной модели нарушителя актуальным нарушителем не является специалист в области разработки

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
		и анализа СКЗИ.
б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;	—	Во всех этапах жизненного цикла СКЗИ участвуют доверенные сотрудники организации. Разработчики и поставщики СКЗИ, признаны неактуальными нарушителями.
в) проведение атаки находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее контролируемая зона);	+	Внешний нарушитель признан актуальным.
г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак: – внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности, представляющие среду функционирования СКЗИ (далее — СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ; – внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ;	— —	Во всех этапах жизненного цикла СКЗИ участвуют доверенные сотрудники организации. Разработчики и поставщики СКЗИ, признаны неактуальными нарушителями.
д) проведение атак на этапе эксплуатации СКЗИ на:		Внешний нарушительпризнан актуальным, поэтому атаки на

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
– персональные данные; – ключевую, аутентифицирующую и парольную информацию СКЗИ; – программные компоненты СКЗИ; – аппаратные компоненты СКЗИ; – программные компоненты СФ, включая программное обеспечение BIOS; – аппаратные компоненты СФ; – данные, передаваемые по каналам связи; – иные объекты, которые установлены при формировании совокупности предложений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее — АС) и программного обеспечения (далее — ПО);	+ — — — + — + —	передаваемые по каналам связи данные и персональные данные субъектовпотенциально могут быть осуществимы. Угрозы атак на остальные объекты признаны неактуальными в силу доверенности сотрудников, сопровождающих СКЗИ на этапе эксплуатации.
е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация: – общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);	+ +	Внешнему нарушителю могут быть доступны только сведения по объектам, полученные из свободных источников.

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
– сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;	—	
– содержание конструкторской документации на СКЗИ;	—	
– содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;	+	
– общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;	+	
– сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее — канал связи);	—	
– все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;	—	
– сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;	—	

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
– сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ; – сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ;	— —	
ж) применение: – находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ; – специально разработанных АС и ПО;	 + —	Внешний нарушитель, признанный актуальным, может использовать АС и ПО, применяемые в системе и находящиеся в свободном доступе или используемые за пределами КЗ, с целью получения дополнительных сведений о функционировании системы.
з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: – каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами; – каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ;	 + —	Внешний нарушитель признан актуальным, каналы связи не защищены должным образом. Угрозы утечки конфиденциальных данных по каналам ПЭМИН, акустическому, виброакустическому, видовому признаны неактуальными.
и) проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей	+	Система имеет выход в ИТС.

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
(далее — ИТС), доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;		
к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства).	+	Внешний нарушитель, признанный актуальным, может использовать АС и ПО, применяемые в АСУ СО ТО с целью получения дополнительных сведений о функционировании системы.
СКЗИ класса КС2		
а) проведение атаки при нахождении в пределах контролируемой зоны (далее – КЗ);	—	Внутренний нарушитель признан неактуальным
б) 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;	— —	Внутренний нарушитель признан неактуальным
в) получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: – сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;	—	В настоящей модели угроз нет актуального нарушителя, имеющего возможность беспрепятственно получить приведенную информацию, внутренний нарушитель признан

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
– сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; – сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;	— —	неактуальным
г) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	—	В настоящей модели угроз нет актуального нарушителя, имеющего возможность использовать штатные средства в целях НСД.
СКЗИ класса КС3		
а) физический доступ к СВТ, на которых реализованы СКЗИ и СФ;	—	В настоящей модели угроз нет актуального нарушителя, способного реализовать перечисленные возможности.
б) возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	—	В настоящей модели угроз нет актуального нарушителя, способного реализовать перечисленные возможности.
СКЗИ класса КВ		
а) 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;	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.

Возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	+/—	Пояснение
б) проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.
в) 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.	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.
СКЗИ класса КА		
а) создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО;	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.
б) возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.
в) возможность располагать всеми аппаратными компонентами СКЗИ и СФ.	—	Актуальный нарушитель, согласно настоящей модели угроз, не располагает перечисленными возможностями.

Согласно Приказу ФСБ №378, для обеспечения **2 уровня защищенности** персональных данных при их обработке в информационной системе и актуальных угрозах 3 типа, должны применяться СКЗИ класса КС1 и выше. Исходя из результатов анализа способов получения исходных данных при создании способов, подготовке и проведении атак злоумышленников (см. Приложение А настоящего документа), для обеспечения

безопасности персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого (далее – атака), должны применяться **СКЗИ класса не ниже КС1**.

ПРИЛОЖЕНИЕ Б. ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ БЕЗОПАСНОСТИ ПДН В АСУ СО ТО *МБУ ДО «ДШИ»*

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.1.	**Угроза автоматического распространения вредоносного кода в грид-системе** Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при малой администрируемостигрид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.2.	**Угроза агрегирования данных, передаваемых в грид-системе** Угроза заключается в возможности раскрытия нарушителем защищаемой информации путём выявления задействованных в её обработке узлов, сбора, анализа и обобщения данных, перехватываемых в сети передачи данных грид-системы. Данная угроза обусловлена слабостью технологии грид-вычислений – использованием незащищённых каналов сети Интернет как транспортной сети грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя: сил и средств, достаточных для компенсации чрезвычайной распределённостигрид-заданий между узлами грид-системы; привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.3.	**Угроза анализа криптографических алгоритмов и их реализации** Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки						
	Отсутствует	Метаданные, системное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.4.	**Угроза аппаратного сброса пароля BIOS** Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы BIOS (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»). Данная угроза обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.5.	**Угроза внедрения вредоносного кода в BIOS** Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.6.	**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 (N1)	Системное, прикладное, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.7.	**Угроза воздействия на программы с высокими привилегиями** Угроза заключается в возможности повышения нарушителем своих привилегий в дискредитированной системе (получения привилегии дискредитированных программ) путём использования ошибок в программах и выполнения произвольного кода с их привилегиями. Данная угроза обусловлена слабостями механизма проверки входных данных и команд, а также мер по разграничению доступа. Реализация данной угрозы возможна при условиях: обладания дискредитируемой программой повышенными привилегиями в системе; осуществления дискредитируемой программой приёма входных данных от других программ или от пользователя; нарушитель имеет возможность осуществлять передачу данных к дискредитируемой программе						
	Отсутствует	Информационная система, сетевое ПО, сетевой трафик	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.8.	**Угроза восстановления аутентификационной информации** Угроза заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе. Данная угроза обусловлена значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой, что определяет два следствия: время подбора в основном определяется не объёмом аутентификационной информации, а объёмом данных её хеш-кода; восстановленная аутентификационная информация может не совпадать с исходной (при применении некоторых алгоритмов для нескольких наборов исходных данных могут быть получены одинаковые результаты – хеш-коды). Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, микропрограммное обеспечение, учётные данные пользователя	Средний	Высокая	Средний	**Актуальна**	
У.9.	**Угроза восстановления предыдущей уязвимой версии BIOS** Угроза заключается в возможности осуществления вынужденного перехода на использование BIOS/UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. При использовании технологии обновления BIOS/UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): на компьютере установлена некоторая версия BIOS/UEFI, для которой на момент её работы не известны уязвимости; в силу некоторых обстоятельств BIOS/UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию BIOS/UEFI на случай «отката» системы; публикуются данные о существовании уязвимостей в предыдущей версии BIOS/UEFI; происходит сбой в работе системы, в результате чего текущая (новая) версия BIOS/UEFI становится неработоспособной (например, нарушается её целостность); пользователь осуществляет штатную процедуру восстановления работоспособности системы – проводит «откат» системы к предыдущему работоспособному состоянию						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.10.	**Угроза выхода процесса за пределы виртуальной машины** Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, 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						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.11.	**Угроза деавторизации санкционированного клиента беспроводной сети** Угроза заключается в возможности автоматического разрыва соединения беспроводной точки доступа с санкционированным клиентом беспроводной сети. Данная угроза обусловлена слабостью технологий сетевого взаимодействия по беспроводным каналам передачи данных – сведения о MAC-адресах беспроводных клиентов доступны всем участникам сетевого взаимодействия. Реализация данной угрозы возможна при условии подключения нарушителем к беспроводной сети устройства, MAC-адрес которого будет полностью совпадать с MAC-адресом дискредитируемого санкционированного клиента						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.12.	**Угроза деструктивного изменения конфигурации/среды окружения программ** Угроза заключается в возможности деструктивного программного воздействия на дискредитируемое приложение путём осуществления манипуляций с используемыми им конфигурационными файлами или библиотеками. Данная угроза обусловлена слабостями мер контроля целостности конфигурационных файлов или библиотек, используемых приложениями. Реализация данной угрозы возможна в случае наличия у нарушителя прав осуществления записи в файловые объекты, связанные с конфигурацией/средой окружения программы, или возможности перенаправления запросов дискредитируемой программы от защищённых файловых объектов к ложным						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Системное, прикладное, сетевое ПО, микропрограммное обеспечение, метаданные, объекты файловой системы, реестр	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.13.	**Угроза деструктивного использования декларированного функционала BIOS** Угроза заключается в возможности неправомерного использования декларированного функционала BIOS/UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения BIOS/UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки целостности памяти, программного обеспечения управления RAID-контроллером и т.п.). Реализации данной угрозы может способствовать возможность обновления некоторых BIOS/UEFI без прохождения аутентификации						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.14.	**Угроза длительного удержания вычислительных ресурсов пользователями** Угроза заключается в возможности ограничения нарушителем доступа конечных пользователей к вычислительному ресурсу за счёт принудительного удержания его в загруженном состоянии путём осуществления им многократного выполнения определённых деструктивных действий или эксплуатации уязвимостей программ, распределяющих вычислительные ресурсы между задачами. Данная угроза обусловлена слабостями механизмов балансировки нагрузки и распределения вычислительных ресурсов. Реализация угрозы возможна в случае, если у нарушителя имеется возможность делать запросы, которые в совокупности требуют больше времени на выполнение, чем запросы пользователя						
	Внешний нарушитель с низким потенциалом (N1)	Информационная система, сетевой узел, носитель информации, системноеи сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.15.	**Угроза доступа к защищаемым файлам с использованием обходного пути** Угроза заключается в возможности получения нарушителем доступа к скрытым/защищаемым каталогам или файлам посредством различных воздействий на файловую систему (добавление дополнительных символов в указании пути к файлу; обращение к файлам, которые явно не указаны в окне приложения). Данная угроза обусловлена слабостями механизма разграничения доступа к объектам файловой системы.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при условиях: наличие у нарушителя прав доступа к некоторым объектам файловой системы; отсутствие проверки вводимых пользователем данных; наличие у дискредитируемой программы слишком высоких привилегий доступа к файлам, обработка которых не предполагается с её помощью						
	Внешний нарушитель с низким потенциалом(N1)	Объекты файловой системы	Средний	Высокая	Средний	**Актуальна**	
У.16.	**Угроза доступа к локальным файлам сервера при помощи URL** Угроза заключается в возможности передачи нарушителем дискредитируемому браузеру запроса на доступ к файловой системе пользователя вместо URL-запроса. При этом браузер выполнит этот запрос с правами, которыми он был наделён при запуске, и передаст данные, полученные в результате выполнения этой операции, нарушителю. Данная угроза обусловлена слабостями механизма проверки вводимых пользователем запросов, который не делает различий между запросами на доступ к файловой системе и URL-запросами. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий на отправку запросов браузеру, функционирующему в дискредитируемой системе						
	Внешний нарушитель с низким потенциалом(N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.17.	**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 их значений со стороны дискредитируемого приложения						
	Внешний нарушитель с низким потенциалом(N1)	Прикладное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.18.	**Угроза загрузки нештатной операционной системы** Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного переконфигурирования в BIOS/UEFI пути доступа к загрузчику операционной системы. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки BIOS/UEFI – указания источника загрузки операционной системы						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	
У.19.	**Угроза заражения DNS-кеша** Угроза заключается в возможности перенаправления нарушителем сетевого трафика через собственный сетевой узел путём опосредованного изменения таблиц соответствия IP- и доменных имён, хранимых в DNS-сервере, за счёт генерации лавины возможных ответов на запрос DNS-сервера легальному пользователю или за счёт эксплуатации уязвимостей DNS-сервера. Данная угроза обусловлена слабостями механизмов проверки подлинности субъектов сетевого взаимодействия, а также уязвимостями DNS-сервера, позволяющими напрямую заменить DNS-кеш DNS-сервера. Реализация данной угрозы возможна в случае наличия у нарушителя привилегий, достаточных для отправки сетевых запросов к DNS-серверу						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.20.	**Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг** Угроза заключается в возможности осуществления потребителем облачных услуг (нарушителем) рассылки спама, несанкционированного доступа к виртуальным машинам других потребителей облачных услуг или осуществления других деструктивных программных воздействий на различные системы с помощью арендованных ресурсов облачного сервера. Данная угроза обусловлена тем, что потребитель облачных услуг может устанавливать собственное программное обеспечение на облачный сервер. Реализация данной угрозы возможна путём установки и запуска потребителем облачных услуг вредоносного программного обеспечения на облачный сервер. Успешная реализация данной угрозы потребителем облачных услуг оказывает негативное влияние на репутацию поставщика облачных услуг						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.21.	**Угроза злоупотребления доверием потребителей облачных услуг** Угроза заключается в возможности нарушения (случайно или намеренно) защищённости информации потребителей облачных услуг внутренними нарушителями поставщика облачных услуг. Данная угроза обусловлена тем, что значительная часть функций безопасности переведена в сферу ответственности поставщика облачных услуг, а также невозможностью принятия потребителем облачных услуг мер защиты от действий сотрудников поставщика облачных услуг. Реализация данной угрозы возможна при условии того, что потребители облачных услуг не входят в состав организации, осуществляющей оказание данных облачных услуг (т.е. потребитель действительно передал поставщику собственную информацию для осуществления её обработки)						
	Внешний нарушитель с низким потенциалом(N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.22.	**Угроза избыточного выделения оперативной памяти** Угроза заключается в возможности выделения значительных ресурсов оперативной памяти для обслуживания запросов вредоносных программ и соответственного снижения объёма ресурсов оперативной памяти, доступных в системе для выделения в ответ на запросы программ легальных пользователей. Данная угроза обусловлена наличием слабостей механизма контроля выделения оперативной памяти различным программам. Реализация данной угрозы возможна при условии нахождения вредоносного программного обеспечения в системе в активном состоянии						
	Внешний нарушитель с низким потенциалом (N1)	Аппаратное обеспечение, системное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.23.	**Угроза изменения компонентов системы** Угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрения закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе						
	Отсутствует	Информационная система, сервер, системное ПО, прикладное ПО, аппаратное	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
		обеспечение					
У.24.	**Угроза изменения режимов работы аппаратных элементов компьютера** Угроза заключается в возможности изменения нарушителем режимов работы аппаратных элементов компьютера путём несанкционированного переконфигурирования BIOS/UEFI, что позволяет: за счёт изменения частоты системной шины, режима передачи данных по каналам связи и т.п. повлиять на общую производительность компьютера или вызвать сбои в его работе; за счёт понижения входного напряжения, отключения систем охлаждения временно обеспечить неработоспособность компьютера; за счёт задания недопустимых параметров работы устройств (порогового значения отключения устройства при перегреве, входного напряжения и т.п.) привести к физическому выходу из строя отдельных аппаратных элементов компьютера. Данная угроза обусловлена слабостями технологий разграничения доступа к управлению BIOS/UEFI. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение соответствующих параметров настройки BIOS/UEFI						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.25.	**Угроза изменения системных и глобальных переменных** Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на некоторые программы или систему в целом путём изменения используемых дискредитируемыми программами единых системных и глобальных переменных. Данная угроза обусловлена слабостями механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к системным и глобальным переменным и отсутствии проверки целостности их значений со стороны дискредитируемого приложения						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.26.	**Угроза искажения XML-схемы** Угроза заключается в возможности изменения нарушителем алгоритма обработки информации приложениями, функционирующими на основе XML-схем, вплоть до приведения приложения в состояние "отказ в обслуживании", путём изменения XML-схемы, передаваемой между клиентом и сервером. Данная угроза обусловлена слабостями мер обеспечения целостности передаваемых при клиент-серверном взаимодействии данных, а также слабостями						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	механизма сетевого взаимодействия открытых систем. Реализация данной угрозы возможна при условиях осуществления нарушителем успешного несанкционированного доступа к сетевому трафику, передаваемому между клиентом и сервером и отсутствии проверки целостности XML-схемы со стороны дискредитируемого приложения						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.27.	**Угроза искажения вводимой и выводимой на периферийные устройства информации** Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём подмены или искажения исходных данных, поступающих от датчиков, клавиатуры или других устройств ввода информации, а также подмены или искажения информации, выводимой на принтер, дисплей оператора или на другие периферийные устройства. Данная угроза обусловлена слабостями мер антивирусной защиты и контроля достоверности входных и выходных данных, а также ошибками, допущенными в ходе проведения специальных проверок аппаратных средств вычислительной техники. Реализация данной угрозы возможна при условии наличия в дискредитируемой информационной системе вредоносного программного обеспечения (например, виртуальных драйверов устройств) или аппаратных закладок						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, аппаратное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.28.	**Угроза использования альтернативных путей доступа к ресурсам** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса). Данная угроза обусловлена слабостями мер разграничения доступа к защищаемой информации, слабостями фильтрации входных данных. Реализация данной угрозы возможна при условии наличия у нарушителя: возможности ввода произвольных данных в адресную строку; сведений о пути к защищаемому ресурсу; возможности изменения интерфейса ввода входных данных						
	Внешний нарушитель с низким потенциалом (N1)	Объекты файловой системы, прикладное ПО, системное ПО	Средний	Высокая	Средний	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.29.	**Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами** Угроза заключается в возможности существенного снижения производительности вычислительного поля суперкомпьютера и эффективности выполнения на нём текущих параллельных вычислений из-за потребления вычислительных ресурсов суперкомпьютера «паразитными» процессами («процессами-потомками» предыдущих заданий или процессами, запущенными вредоносным программным обеспечением). Данная угроза обусловлена слабостями мер очистки памяти от «процессов-потомков» завершённых заданий, а также процессов, запущенных вредоносным программным обеспечением. Реализация данной угрозы возможна при условии некорректного завершения выполненных задач или наличия вредоносных процессов в памяти суперкомпьютера в активном состоянии						
	Внешний нарушитель с низким потенциалом(N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.30.	**Угроза использования информации идентификации/аутентификации, заданной по умолчанию** Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты. Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset). Реализация данной угрозы возможна при одном из следующих условий: наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты; успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты						
	Внешний нарушитель с низким потенциалом (N1)	Средства защиты информации, системное ПО, сетевое ПО, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты	Средний	Высокая	Средний	**Актуальна**	
У.31.	**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.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, прикладное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.32.	**Угроза использования поддельных цифровых подписей BIOS** Угроза заключается в возможности установки уязвимой версии обновления BIOS/UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер по контролю за благонадёжностью центров выдачи цифровых подписей. Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления BIOS/UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.33.	**Угроза использования слабостей кодирования входных данных** Угроза заключается в возможности осуществления нарушителем деструктивного информационного воздействия на дискредитируемую систему путём манипулирования значениями входных данных и формой их предоставления (альтернативные кодировки, некорректное расширение файлов и т.п.). Данная угроза обусловлена слабостями механизма контроля входных данных. Реализация данной угрозы возможна при условиях: дискредитируемая система принимает входные данные от нарушителя; нарушитель обладает возможностью управления одним или несколькими параметрами входных данных						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.34.	**Угроза использования слабостей протоколов сетевого/локального обмена данными** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к передаваемой в системе защищаемой информации за счёт деструктивного воздействия на протоколы сетевого/локального обмена данными в системе путём нарушения правил использования данных протоколов. Данная угроза обусловлена слабостями самих протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.35.	**Угроза использования слабых криптографических алгоритмов BIOS** Угроза заключается в сложности проверки реальных параметров работы и алгоритмов, реализованных в криптографических средствах BIOS/UEFI. При этом доверие к криптографической защите будет ограничено доверием к производителю BIOS. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении BIOS/UEFI. Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.36.	**Угроза исследования механизмов работы программы** Угроза заключается в возможности проведения нарушителем обратного инжиниринга кода программы и дальнейшего исследования его структуры, функционала и состава в интересах определения алгоритма работы программы и поиска в ней уязвимостей. Данная угроза обусловлена слабостями механизма защиты кода программы от исследования. Реализация данной угрозы возможна в случаях: наличия у нарушителя доступа к исходным файлам программы; наличия у нарушителя доступа к дистрибутиву программы и отсутствия механизма защиты кода программы от исследования						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.37.	**Угроза исследования приложения через отчёты об ошибках** Угроза заключается в возможности исследования нарушителем алгоритма работы дискредитируемого приложения и его предполагаемой структуры путём анализа генерируемых этим приложением отчётов об ошибках. Данная угроза обусловлена размещением защищаемой информации (или информации, обобщение которой может раскрыть защищаемые сведения о системе) в генерируемых отчётах об ошибках. Реализация данной угрозы возможна в случае наличия у нарушителя доступа к отчётам об ошибках, генерируемых приложением, и наличия избыточности содержащихся в них данных						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.38.	**Угроза исчерпания вычислительных ресурсов хранилища больших данных** Угроза заключается в возможности временного возникновения состояния типа «отказ в обслуживании» у хранилища больших данных. Данная угроза обусловлена постоянным трудно контролируемым заполнением занятого дискового пространства за счёт данных, непрерывно поступающих из различных информационных источников, и слабостями технологий доступа и хранения информации в хранилищах больших данных. Реализация данной угрозы возможна при условии мгновенного (текущего) превышения скорости передачи данных над скоростью их сохранения (в силу недостаточности пропускной способности канала связи или скорости выделения свободного пространства и сохранения на него поступающих данных) или при условии временного отсутствия свободного места в хранилище (в силу некорректного управления хранилищем или в результате осуществления нарушителем деструктивного программного воздействия на механизм контроля за заполнением хранилища путём изменения параметров или логики его работы)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.39.	**Угроза исчерпания запаса ключей, необходимых для обновления BIOS** Угроза заключается в возможности нарушения (невозможности осуществления) процедуры обновления BIOS/UEFI при исчерпании запаса необходимых для её проведения ключей. Данная угроза обусловлена ограниченностью набора ключей, необходимых для обновления BIOS/UEFI. Реализация данной угрозы возможна путём эксплуатации уязвимостей средств обновления набора ключей, или путём использования нарушителем программных средств перебора ключей						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.40.	**Угроза конфликта юрисдикций различных стран** Угроза заключается в возможности отказа в трансграничной передаче защищаемой информации в рамках оказания облачных услуг в соответствии с требованиями локального законодательства стран, резиденты которых участвуют в оказании облачных услуг. Данная угроза обусловлена тем, что в зависимости от особенностей законодательства различных стран, резиденты которых участвуют в оказании облачных услуг, при обеспечении информационной безопасности могут использоваться правовые меры различных юрисдикций.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при условии того, что на обеспечение информационной безопасности в ходе оказания облачных услуг накладываются правовые меры различных юрисдикций, противоречащих друг другу в ряде вопросов						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.41.	**Угроза межсайтового скриптинга** Угроза заключается в возможности внедрения нарушителем участков вредоносного кода на сайт дискредитируемой системы таким образом, что он будет выполнен на рабочей станции просматривающего этот сайт пользователя. Данная угроза обусловлена слабостями механизма проверки безопасности при обработке запросов и данных, поступающих от веб-сайта. Реализация угрозы возможна в случае, если клиентское программное обеспечение поддерживает выполнение сценариев, а нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.42.	**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 низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.43.	**Угроза нарушения доступности облачного сервера** Угроза заключается в возможности прекращения оказания облачных услуг всем потребителям (или группе потребителей) из-за нарушения доступности для них облачной инфраструктуры. Данная угроза обусловлена тем, что обеспечение доступности не является специфичным требованием безопасности информации для облачных технологий, и, кроме того, облачные системы реализованы в соответствии с сервис-ориентированным подходом. Реализация данной угрозы возможна при переходе одного или нескольких облачных серверов в состояние «отказ в обслуживании». Более того, способность динамически изменять объём предоставляемых потребителям облачных услуг может быть использована нарушителем для реализации угрозы. При этом						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.44.	**Угроза нарушения изоляции пользовательских данных внутри виртуальной машины** Угроза заключается в возможности нарушения безопасности пользовательских данных программ, функционирующих внутри виртуальной машины, вредоносным программным обеспечением, функционирующим вне виртуальной машины. Данная угроза обусловлена наличием уязвимостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри виртуальной машины, от несанкционированного доступа со стороны вредоносного программного обеспечения, функционирующего вне виртуальной машины. Реализация данной угрозы возможна при условии успешного преодоления вредоносным программным кодом границ виртуальной машины не только за счёт эксплуатации уязвимостей гипервизора, но и путём осуществления такого воздействия с более низких (по отношению к гипервизору) уровней функционирования системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.45.	**Угроза нарушения изоляции среды исполнения BIOS** Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения BIOS/UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к BIOS/UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи. Реализация данной угрозы возможна: со стороны операционной системы – при условии наличия BIOS/UEFI функционала обновления и (или) управления программным обеспечением BIOS/UEFI из операционной системы; со стороны сети – при условии наличия у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию BIOS/UEFI серверов системы, и дискредитируемого сервера						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.46.	**Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия** Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия. Данная угроза обусловлена наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между её уровнями. Реализация данной угрозы возможна в случае возникновения ошибок при проведении аутентификации субъектов виртуального информационного взаимодействия						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.47.	**Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке** Угроза заключается в возможности значительного снижения производительности грид-системы, вплоть до временного нарушения её работоспособности при появлении нетипичной сетевой нагрузки (в т.ч. вызванной распределённой DoS-атакой, активностью других пользователей в сети и др.). Данная угроза обусловлена слабостью технологий грид-вычислений – производительность грид-системы имеет сильную зависимость от загруженности каналов связи, что является следствием максимальной территориальной распределённости вычислительного модуля грид-системы среди всех типов информационных систем. Реализация данной угрозы возможна при условии недостаточного контроля за состоянием отдельных узлов грид-системы со стороны диспетчера задач грид-системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.48.	**Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин** Угроза заключается в возможности осуществления деструктивного программного воздействия на дискредитируемую систему или опосредованного деструктивного программного воздействия через неё на другие системы путём осуществления несанкционированного доступа к образам виртуальных машин. Данная угроза обусловлена слабостями мер разграничения доступа к образам виртуальных машин, реализованных в программном обеспечении виртуализации. Реализация данной угрозы может привести: к нарушению конфиденциальности защищаемой информации, обрабатываемой с помощью виртуальных машин, созданных на основе несанкционированно изменённых образов;						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	к нарушению целостности программ, установленных на виртуальных машинах; к нарушению доступности ресурсов виртуальных машин; к созданию ботнета путём внедрения вредоносного программного обеспечения в образы виртуальных машин, используемые в качестве шаблонов (эталонные образы)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.49.	**Угроза нарушения целостности данных кеша** Угроза заключается в возможности размещения нарушителем в кеше приложения (например, браузера) или службы (например, DNS или ARP) некорректных (потенциально опасных) данных таким образом, что до обновления кеша дискредитируемое приложение (или служба) будет считать эти данные корректными. Данная угроза обусловлена слабостями в механизме контроля целостности данных в кеше. Реализация данной угрозы возможна в условиях осуществления нарушителем успешного несанкционированного доступа к данным кеша и отсутствии проверки целостности данных в кеше со стороны дискредитируемого приложения (или службы)						
	Внешний нарушитель с низким потенциалом(N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.50.	**Угроза неверного определения формата входных данных, поступающих в хранилище больших данных** Угроза заключается в возможности искажения информации, сохраняемой в хранилище больших данных, или отказа в проведении сохранения при передаче в него данных в некоторых форматах. Данная угроза обусловлена слабостями технологий определения формата входных данных на основе дополнительной служебной информации (заголовки файлов и сетевых пакетов, расширения файлов и т.п.), а также технологий адаптивного выбора и применения методов обработки мультиформатной информации в хранилищах больших данных. Реализация данной угрозы возможна при условии, что дополнительная служебная информация о данных по какой-либо причине не соответствует их фактическому содержимому, или в хранилище больших данных не реализованы методы обработки данных получаемого формата						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.51.	**Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания** Угроза заключается в возможности потери несохранённых данных, обрабатываемых в предыдущей сессии работы на компьютере, а также в возможности потери времени для возобновления работы на компьютере. Данная угроза обусловлена ошибками в реализации программно-аппаратных компонентов компьютера, связанных с обеспечением питания. Реализация данной угрозы возможна при условии невозможности выведения компьютера из промежуточных состояний питания («ждущего режима работы», «гибернации» и др.)						
	Отсутствует	Носитель информации, системное ПО, метаданные, объекты файловой системы, реестр	Средний	-	-	**Неактуальна**	
У.52.	**Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения** Угроза заключается в возможности возникновения у потребителя облачных услуг непреодолимых сложностей для смены поставщика облачных услуг из-за технических сложностей в реализации процедуры миграции образов виртуальных машин из облачной системы одного поставщика облачных услуг в систему другого. Данная угроза обусловлена тем, что каждый поставщик облачных услуг использует для реализации своей деятельности аппаратное и программное обеспечение различных производителей, часть которого может использовать специфические (для данного производителя) инструкции, протоколы, методы, схемы коммутации и другие особенности реализации своего функционала. Реализация данной угрозы возможна в случае несовместимости стандартных программных интерфейсов обмена данными (API) для реализации процедуры миграции образов виртуальных машин между различными поставщиками облачных услуг в одном или обоих направлениях. Также данная угроза обуславливает ограничение возможности смены производителей аппаратного и программного обеспечения поставщиком облачных услуг, что может привести к нарушению целостности и доступности информации по вине поставщика облачных услуг						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.53.	**Угроза невозможности управления правами пользователей BIOS** Угроза заключается в возможности неправомерного использования пользователями декларированного функционала BIOS/UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу BIOS/UEFI между различными пользователями и администраторами. Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.54.	**Угроза недобросовестного исполнения обязательств поставщиками облачных услуг** Угроза заключается в возможности раскрытия или повреждения 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.						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.55.	**Угроза незащищённого администрирования облачных услуг** Угроза заключается в возможности осуществления опосредованного деструктивного программного воздействия на часть или все информационные системы, функционирующие в облачной среде, путём перехвата управления над облачной инфраструктурой через механизмы удалённого администрирования. Данная угроза обусловлена недостаточностью внимания, уделяемого контролю вводимых пользователями облачных услуг данных (в том числе аутентификационных данных), а также уязвимостями небезопасных интерфейсов обмена данными (API), используемых средствами удалённого администрирования. Реализация данной угрозы возможна в случае получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.56.	**Угроза некачественного переноса инфраструктуры в облако** Угроза заключается в возможности снижения реального уровня защищённости иммигрирующей в облако информационной системы из-за ошибок, допущенных при миграции в ходе преобразования её реальной инфраструктуры в облачную. Данная угроза обусловлена тем, что преобразование даже части инфраструктуры информационной системы в облачную зачастую требует проведения серьёзных изменений в такой инфраструктуре (например, в политиках безопасности и организации сетевого обмена данными). Реализация данной угрозы возможна в случае несовместимости программных и сетевых интерфейсов или несоответствий политик безопасности при						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	осуществлении переноса информационной системы в облако						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.57.	**Угроза неконтролируемого копирования данных внутри хранилища больших данных** Угроза заключается в сложности контроля за всеми автоматически создаваемыми копиями информации в хранилище больших данных из-за временной несогласованности данных операций. Данная угроза обусловлена осуществлением дублирования (дву- или многократного) данных на различных вычислительных узлах, входящих в состав хранилища больших данных, с целью повышения скорости доступа к этим данным при большом количестве запросов чтения/записи. При этом данная операция является внутренней функцией и «непрозрачна» для конечных пользователей и администраторов хранилища больших данных. Реализация данной угрозы возможна при условии недостаточности мер по контролю за автоматически создаваемыми копиями информации, применяемых в хранилище больших данных						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.58.	**Угроза неконтролируемого роста числа виртуальных машин** Угроза заключается в возможности ограничения или нарушения доступности виртуальных ресурсов для конечных потребителей облачных услуг путём случайного или несанкционированного преднамеренного создания нарушителем множества виртуальных машин. Данная угроза обусловлена ограниченностью объёма дискового пространства, выделенного под виртуальную инфраструктуру, и слабостями технологий контроля процесса создания виртуальных машин. Реализация данной угрозы возможна при условии наличия у нарушителя прав на создание виртуальных машин в облачной инфраструктуре						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.59.	**Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов** Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти).						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена уязвимостями программного обеспечения уровня управления виртуальной инфраструктурой, реализующего функцию распределения компьютерных ресурсов между пользователями. Реализация данной угрозы возможна при условии успешного осуществления нарушителем несанкционированного доступа к программному обеспечению уровня управления виртуальной инфраструктурой, реализующему функцию распределения компьютерных ресурсов между пользователями						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.60.	**Угроза неконтролируемого уничтожения информации хранилищем больших данных** Угроза заключается в возможности удаления из хранилища некоторых обрабатываемых данных без уведомления конечного пользователя или администратора. Данная угроза обусловлена слабостями механизма автоматического удаления данных, не отвечающих определённым требованиям (предельный «срок жизни» в хранилище, конечная несогласованность с другими данными, создание копии в другом месте и т.п.). Реализация данной угрозы возможна при условии недостаточности реализованных в хранилище больших данных мер по контролю за автоматическим удалением данных						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.61.	**Угроза некорректного задания структуры данных транзакции** Угроза заключается в возможности совершения нарушителем (клиентом базы данных) подлога путём прерывания транзакции или подмены идентификатора транзакции. В первом случае происходит неполное выполнение транзакции, а во втором – пользователь форсированно завершает транзакцию, изменяя её ID, и сообщая о том, что транзакция не была проведена, тем самым провоцируя повторное проведение транзакции. Данная угроза обусловлена слабостями механизма контроля непрерывности транзакций и целостности данных, передаваемых в ходе транзакции между базой данных и её клиентом						
	Отсутствует	Сетевой трафик, база данных, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.62.	**Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера** Угроза заключается в возможности перенаправления или копирования обрабатываемых браузером данных через прозрачный прокси-сервер, подключённый к						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	браузеру в качестве плагина. Данная угроза обусловлена слабостями механизма контроля доступа к настройкам браузера. Реализация возможна в случае успешного осуществления нарушителем включения режима использования прозрачного прокси-сервера в параметрах настройки браузера, например, в результате реализации угрозы межсайтового скриптинга						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.63.	**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						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, аппаратное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.64.	**Угроза некорректной реализации политики лицензирования в облаке** Угроза заключается в возможности отказа потребителям облачных услуг в удалённом доступе к арендуемому программному обеспечению (т.е. происходит потеря доступности облачной услуги SaaS) по вине поставщика облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками лицензирования использования программного обеспечения различных производителей в облаке. Реализация данной угрозы возможна при условии, что политика лицензирования использования программного обеспечения основана на ограничении количества его установок или числа его пользователей, а созданные виртуальные машины с лицензируемым программным обеспечением использованы много раз						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствуют	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.65.	**Угроза неопределённости в распределении ответственности между ролями в облаке** Угроза заключается в возможности возникновения существенных разногласий между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей в части обеспечения информационной безопасности.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена отсутствием достаточного набора мер контроля за распределением ответственности между различными ролями в части владения данными, контроля доступа, поддержки облачной инфраструктуры и т. п. Возможность реализации данной угрозы повышается в случае использования облачных услуг, предоставляемых другими поставщиками (т.е. в случае использования схемы оказания облачных услуг с участием посредников)						
	Внешний нарушитель с низким потенциалом(N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.66.	**Угроза неопределённости ответственности за обеспечение безопасности облака** Угроза заключается в возможности невыполнения ряда мер по защите информации как поставщиком облачных услуг, так и их потребителем. Данная угроза обусловлена отсутствием чёткого разделения ответственности в части обеспечения безопасности информации между потребителем и поставщиком облачных услуг. Реализация данной угрозы возможна при условии недостаточности документального разделения сфер ответственности между сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.67.	**Угроза неправомерного ознакомления с защищаемой информацией** Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Данная угроза обусловлена уязвимостями средств контроля доступа, ошибками в параметрах конфигурации данных средств или отсутствием указанных средств. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.						
	Отсутствует	Аппаратное обеспечение, носители информации, объекты файловой системы	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.68.	**Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением** Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на API в целях реализации функций, изначально не предусмотренных дискредитируемым приложением (например, использование функций отладки из состава API).						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	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						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.69.	**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 (N1)	Сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.70.	**Угроза непрерывной модернизации облачной инфраструктуры** Угроза заключается в возможности занесения в облачную систему уязвимостей и слабостей вместе с добавлением нового программного или аппаратного обеспечения. При этом система, рассматриваемая как защищённая на этапе ввода её в эксплуатацию, уже не может считаться таковой после её модернизации. Данная угроза обусловлена тем, что, во-первых, поставщики облачных услуг предоставляют возможность осуществления потребителем облачных услуг выбора и (или) изменения первоначального состава программного обеспечения облачной инфраструктуры в процессе оказания таких услуг, а, во-вторых, при интенсивном подключении новых потребителей модернизация облачной инфраструктуры может проходить несколько раз в год. Реализация данной угрозы возможна в случае, если срок до следующей модернизации не превышает срока проведения оценки соответствия системы требованиям безопасности в условиях отсутствия системы менеджмента облачных услуг и обеспечения их безопасности (системы облачного менеджмента)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.71.	**Угроза несанкционированного восстановления удалённой защищаемой информации**						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Угроза заключается в возможности осуществления прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановления данных по считанной с машинного носителя остаточной информации. Данная угроза обусловлена слабостями механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Реализация данной угрозы возможна при следующих условиях: удаление информации с машинного носителя происходило без использования способов (методов, алгоритмов) гарантированного стирания данных (например, физическое уничтожение машинного носителя информации); технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных; информация не хранилась в криптографически преобразованном виде						
	Внешний нарушитель с низким потенциалом (N1)	Машинный носитель информации	Средний	Высокая	Средний	**Актуальна**	
У.72.	**Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS** Угроза заключается в возможности внедрения в BIOS/UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в BIOS/UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостями механизма обновления BIOS/UEFI, приводящими к переполнению буфера. Реализация данной угрозы возможна в одном из следующих условий: выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.73.	**Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети** Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путём 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.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования						
	Отсутствует	Сетевое оборудование, микропрограммное обеспечение, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.74.	**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						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, объекты файловой системы, учётные данные пользователя, реестр, машинные носители информации	Средний	Высокая	Средний	**Актуальна**	
У.75.	**Угроза несанкционированного доступа к виртуальным каналам передачи** Угроза заключается в возможности осуществления нарушителем несанкционированного перехвата трафика сетевых узлов, недоступных с помощью сетевых технологий, отличных от сетевых технологий виртуализации, путём некорректного использования таких технологий. Данная угроза обусловлена слабостями мер контроля потоков, межсетевого экранирования и разграничения доступа, реализованных в отношении сетевых технологий виртуализации (с помощью которых строятся виртуальные каналы передачи данных). Реализация данной угрозы возможна при наличии у нарушителя привилегий на осуществление взаимодействия с помощью сетевых технологий виртуализации						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.76.	**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 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,						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	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						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.77.	**Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение** Угроза заключается в возможности нарушения вредоносной программой, функционирующей внутри виртуальной машины, целостности программного кода своей и (или) других виртуальных машин, функционирующих под управлением того же гипервизора, а также изменения параметров её (их) настройки. Данная угроза обусловлена наличием слабостей программного обеспечения гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины. Реализация данной угрозы возможна при условии успешного осуществления несанкционированного доступа со стороны вредоносной программы, функционирующей внутри виртуальной машины, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной виртуальной машины						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.78.	**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 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						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.79.	**Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин** Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе. Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для различные механизмы обмена данными между виртуальными машинами, реализованные в гипервизоре и активированные в системе						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.80.	**Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети** Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической сети с помощью различных сетевых технологий, используемых для осуществления обмена данными в системе, построенной с использованием технологий виртуализации. Данная угроза обусловлена наличием слабостей в сетевых программных интерфейсах гипервизоров, предназначенных для удалённого управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий достаточных для осуществления обмена данными в системе, построенной с использованием технологий виртуализации						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.81.	**Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы** Угроза заключается в возможности выполнения нарушителем сетевого входа на узел грид-системы с правами одной из учётных записей, соответствующей						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	программным процессам системы управления заданиями, с последующим получением доступа к закрытой части криптографических сертификатов, используемых для установления связи в грид-системе. Данная угроза обусловлена наличием уязвимостей в клиенте грид-системы (клиентского программного обеспечения, устанавливаемого в узлах грид-системы), эксплуатация которых позволяет нарушителю осуществлять операции чтения и записи в объектах локальной файловой системы компьютера, отправку сигналов программным процессам (включая сигналы прекращения работы), операции чтения и записи в память программных процессов, соответствующих связующему программному обеспечению и грид-заданиям, открытия сетевых соединений в локальных и внешних узлах грид-системы. Реализация данной угрозы возможна при условии внедрения вредоносного программного кода в систему управления заданиями. Фактически наличие в узле грид-системы неизвестного его владельцу программного обеспечения (клиента грид-системы), проводящего неизвестные вычисления, является «черным ящиком», через который (путём эксплуатации уязвимостей или программных закладок) нарушитель может осуществить противоправные действия по отношению к хранящейся в узле грид-системы защищаемой информации (личной информации владельца узла)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.82.	**Угроза несанкционированного доступа к сегментам вычислительного поля** Угроза заключается в возможности осуществления несанкционированного доступа нарушителя к исходным данным, промежуточным и окончательным результатам расчётов других пользователей суперкомпьютера, а также случайное или преднамеренное деструктивное воздействие процессов решения одних задач на процессы и результаты решения других вычислительных задач. Данная угроза обусловлена слабостями механизма разграничения доступа субъектов к сегментам вычислительных полей суперкомпьютера. Реализация данной угрозы возможна при выполнении задач различных пользователей суперкомпьютера на одном вычислительном поле суперкомпьютера						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.83.	**Угроза несанкционированного доступа к системе по беспроводным каналам** Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в её составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2), используемых для авторизации пользователей при подключении к точке беспроводного доступа. Реализация данной угрозы возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	эксплуатации уязвимостей протоколов идентификации/аутентификации беспроводных сетей, а также нахождения в точке приёма сигналов дискредитируемой беспроводной сети						
	Внешний нарушитель с низким потенциалом (N1)	Учётные данные пользователя, сетевой трафик, аппаратное обеспечение	Средний	Высокая	Средний	**Актуальна**	
У.84.	**Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети** Угроза заключается в возможности осуществления деструктивного программного воздействия на виртуальные устройства хранения данных и (или) виртуальные диски (являющиеся как сегментами виртуального дискового пространства, созданного отдельным виртуальным устройством, так и единым виртуальным дисковым пространством, созданным путём логического объединения нескольких виртуальных устройств хранения данных). Данная угроза обусловлена наличием слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и (или) виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны с высокой сложностью алгоритмов обеспечения согласованности действий по распределению информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства. Реализация данной угрозы возможна при условии наличия у нарушителя специальных программных средств, способных эксплуатировать слабостей технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.85.	**Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации** Угроза заключается в возможности нарушения конфиденциальности информации, содержащейся в распределённых файлах, содержащих защищаемую информацию, путём восстановления данных распределённых файлов из их множества отдельных фрагментов с помощью программного обеспечения и информационных технологий по обработке распределённой информации. Данная угроза обусловлена тем, что в связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Реализация данной угрозы возможна при условии недостаточности или отсутствия мер по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							Данная технология не применяется в ИС
У.86.	**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						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, объекты файловой системы, учётные данные пользователя, реестр	Средний	Высокая	Средний	**Актуальна**	
У.87.	**Угроза несанкционированного использования привилегированных функций BIOS** Угроза заключается в возможности использования нарушителем потенциально опасных возможностей BIOS/UEFI. Данная угроза обусловлена наличием в BIOS/UEFI потенциально опасного функционала						
	Отсутствует	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.88.	**Угроза несанкционированного копирования защищаемой информации** Угроза заключается в возможности неправомерного получения нарушителем копии защищаемой информации путём проведения последовательности неправомерных действий, включающих: несанкционированный доступ к защищаемой информации, копирование найденной информации на съёмный носитель (или в другое место, доступное нарушителю вне системы). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации и контроля доступа лиц в контролируемой зоне. Реализация данной угрозы возможна в случае отсутствия криптографических мер защиты или снятия копии в момент обработки защищаемой информации в нешифрованном виде						
	Внешний нарушитель с низким потенциалом (N1)	Объекты файловой системы, машинный носитель информации	Средний	Высокая	Средний	**Актуальна**	
У.89.	**Угроза несанкционированного редактирования реестра**						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Угроза заключается в возможности внесения нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы MicrosoftWindows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью. Данная угроза обусловлена слабостями механизма контроля доступа, заключающимися в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Реализация данной угрозы возможна в случае получения нарушителем прав на работу с программой редактирования реестра						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, использующее реестр, реестр	Средний	Высокая	Средний	**Актуальна**	
У.90.	**Угроза несанкционированного создания учётной записи пользователя** Угроза заключается в возможности создания нарушителем в системе дополнительной учётной записи пользователя и её дальнейшего использования в собственных неправомерных целях (входа в систему с правами этой учётной записи и осуществления деструктивных действий по отношению к дискредитированной системе или из дискредитированной системы по отношению к другим системам). Данная угроза обусловлена слабостями механизмов разграничения доступа к защищаемой информации. Реализация данной угрозы возможна в случае наличия и прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО	Средний	Высокая	Средний	**Актуальна**	
У.91.	**Угроза несанкционированного удаления защищаемой информации** Угроза заключается в возможности причинения нарушителем экономического, информационного, морального и других видов ущерба собственнику и оператору неправомерно удаляемой информации путём осуществления деструктивного программного или физического воздействия на машинный носитель информации. Данная угроза обусловлена недостаточностью мер по обеспечению доступности защищаемой информации в системе, а равно и наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна в случае получения нарушителем системных прав на стирание данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия						
	Внешний нарушитель с низким потенциалом (N1)	Метаданные, объекты файловой системы, реестр	Средний	Высокая	Средний	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.92.	**Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам** Угроза заключается в возможности получения нарушителем привилегий управления системой путём использования удалённого внеполосного (по независимому вспомогательному каналу TCP/IP) доступа. Данная угроза обусловлена невозможностью контроля за механизмом, реализующего функции удалённого доступа на аппаратном уровне, на уровне операционной системы, а также независимостью от состояния питания аппаратных устройств, т.к. данный механизм предусматривает процедуру удалённого включения/выключения аппаратных устройств. Реализация данной угрозы возможна в условиях: наличия в системе аппаратного обеспечения, поддерживающего технологию удалённого внеполосного доступа; наличия подключения системы к сетям общего пользования (сети Интернет)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Отсутствует актуальный нарушитель, способный осуществить угрозу
У.93.	**Угроза несанкционированного управления буфером** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществления деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода). Данная угроза обусловлена слабостями в механизме разграничения доступа к буферу обмена, а также слабостями в механизмах проверки вводимых данных. Реализация данной угрозы возможна в случае осуществления нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, прикладное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.94.	**Угроза несанкционированного управления синхронизацией и состоянием** Угроза заключается в возможности изменения нарушителей последовательности действий, выполняемых дискредитируемыми приложениями, использующими в своей работе технологии управления процессами на основе текущего времени и состояния информационной системы (например, текущих значений глобальных переменных, наличия запущенных процессов и др.). Данная угроза основана на слабостях механизма управления синхронизацией и состоянием, позволяющих нарушителю вносить изменения в его работу в определённые промежутки времени.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при условии наличия у нарушителя возможности: контролировать состояние дискредитируемого приложения (этапы выполнения алгоритма); отслеживать моменты времени, когда дискредитируемое приложение временно прерывает свою работу с глобальными данными; выполнить деструктивные действия в определённые моменты времени (например, внести изменения в файл с данными или изменить содержимое ячейки памяти)						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.95.	**Угроза несанкционированного управления указателями** Угроза заключается в возможности выполнения нарушителем произвольного вредоносного кода от имени дискредитируемого приложения или приведения дискредитируемого приложения в состояние «отказ в обслуживании» путём изменения указателей на ячейки памяти, содержащие определённые данные, используемые дискредитируемым приложением. Данная угроза связана с уязвимостями в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение указателей, используемых дискредитируемым приложением						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.96.	**Угроза несогласованности политик безопасности элементов облачной инфраструктуры** Угроза заключается в возможности осуществления нарушителем деструктивных программных воздействий как в отношении поставщиков, так и потребителей облачных услуг. Данная угроза обусловлена недостаточностью проработки вопроса управления политиками безопасности элементов облачной инфраструктуры вследствие значительной распределённости облачной инфраструктуры. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)						
	Внешний нарушитель с низким потенциалом(N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.97.	**Угроза несогласованности правил доступа к большим данным** Угроза заключается в возможности предоставления ошибочного неправомерного доступа к защищаемой информации или, наоборот, возможности отказа в доступе к защищаемой информации легальным пользователям в силу ошибок, допущенных при делегировании им привилегий другими легальными						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	пользователями хранилища больших данных. Данная угроза обусловлена недостаточностью мер по разграничению и согласованию доступа к информации различных пользователей в хранилище больших данных. Реализация данной угрозы возможна при условии использования различных политик безопасности, несогласованных между собой (например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.98.	**Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб** Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы (т.н. сканирование портов) для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов. Данная угроза связана с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции сканирования портов и анализа сетевого трафика						
	Внешний нарушитель с низким потенциалом (N1)	Сетевой узел, сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.99.	**Угроза обнаружения хостов** Угроза заключается в возможности сканирования нарушителем вычислительной сети для выявления работающих сетевых узлов. Данная угроза связана со слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями и ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в дискредитируемой системе. Реализация данной угрозы возможна при условии наличия у нарушителя подключения к дискредитируемой вычислительной сети и специализированного программного обеспечения, реализующего функции анализа сетевого трафика						
	Внешний нарушитель с низким потенциалом	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	(N1)						
У.100.	**Угроза обхода некорректно настроенных механизмов аутентификации** Угроза заключается в возможности получения нарушителем привилегий в системе без прохождения процедуры аутентификации за счёт выполнения действий, нарушающих условия корректной работы средств аутентификации (например, ввод данных неподдерживаемого формата). Данная угроза обусловлена в случае некорректных значений параметров конфигурации средств аутентификации и/или отсутствием контроля входных данных. Реализация данной угрозы возможна при условии наличия ошибок в заданных значениях параметров настройки механизмов аутентификации						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.101.	**Угроза общедоступности облачной инфраструктуры** Угроза заключается в возможности осуществления несанкционированного доступа к защищаемой информации одного потребителя облачных услуг со стороны другого. Данная угроза обусловлена тем, что из-за особенностей облачных технологий потребителям облачных услуг приходится совместно использовать одну и ту же облачную инфраструктуру. Реализация данной угрозы возможна в случае допущения ошибок при разделении элементов облачной инфраструктуры между потребителями облачных услуг, а также при изоляции их ресурсов и обособлении данных друг от друга						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.102.	**Угроза опосредованного управления группой программ через совместно используемые данные** Угроза заключается в возможности опосредованного изменения нарушителем алгоритма работы группы программ, использующих одновременно общие данные, через перехват управления над одной из них (ячейки оперативной памяти, глобальные переменные, файлы конфигурации и др.). Данная угроза обусловлена наличием слабостей в механизме контроля внесённых изменений в общие данные каждой из программ в группе. Реализация данной угрозы возможна в случае успешного перехвата нарушителем управления над одной из программ в группе программ, использующих общие данные						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							осуществить угрозу
У.103.	**Угроза определения типов объектов защиты** Угроза заключается в возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (данный метод известен как «fingerprinting», с англ. «дактилоскопия»). Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз. Данная угроза обусловлена ошибками в параметрах конфигурации средств межсетевого экранирования, а также с отсутствием механизмов контроля входных и выходных данных. Реализация данной угрозы возможна в случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией дискредитируемой системы (документация на программные средства, стандарты передачи данных, спецификации и т.п.)						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.104.	**Угроза определения топологии вычислительной сети** Угроза заключается в это механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с уязвимостями средств межсетевого экранирования (алгоритма работы и конфигурации правил фильтрации сетевого трафика). Реализация данной угрозы возможна в случае наличия у нарушителя возможности подключения к исследуемой вычислительной сети и наличием специализированного программного обеспечения, реализующего функцию анализа сетевого трафика						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.105.	**Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных** Угроза заключается в возможности отказа хранилищем больших данных в приёме входных данных неизвестного формата от легального пользователя. Данная угроза обусловлена отсутствием в хранилище больших данных механизма самостоятельной (автоматической) адаптации к новым форматам данных. Реализация данной угрозы возможна при условии поступления запроса на загрузку в хранилище входных данных неизвестного формата						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.106.	**Угроза отказа в обслуживании системой хранения данных суперкомпьютера** Угроза заключается в возможности значительного замедления работы терминальных сессий всех пользователей суперкомпьютера, вплоть до достижения всем суперкомпьютером состояния «отказ в обслуживании» при превышении максимально достижимой нагрузки на параллельную файловую систему суперкомпьютера. Данная угроза обусловлена значительным повышением числа и объёма сохраняемых на накопитель данных для некоторых вычислительных задач. Реализация данной угрозы возможна при условии интенсивного файлового ввода-вывода в кластерной файловой подсистеме суперкомпьютера, основанной на использовании параллельной файловой системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.107.	**Угроза отключения контрольных датчиков** Угроза заключается в возможности обеспечения нарушителем информационной изоляции системы безопасности путём прерывания канала связи с контрольными датчиками, следящими за параметрами состояния системы, или нарушения работы самих датчиков. При этом система перестанет реагировать как на инциденты безопасности (если отключённые датчики являлись частью системы безопасности, например, датчики движения), так и на другие типы инцидентов (например, при отключении датчиков пожарной сигнализации, повышения давления в гидроагрегатах и др.). Данная угроза обусловлена слабостями мер защиты информации в автоматизированных системах управления технологическими процессами, а также наличием уязвимостей в программном обеспечении, реализующим данные меры. Реализация данной угрозы возможна при условии получения доступа (физического или программного) к линиям связи системы безопасности с контрольными датчиками или к самим датчикам						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.108.	**Угроза ошибки обновления гипервизора** Угроза заключается в возможности дискредитации нарушителем функционирующих на базе гипервизора защитных механизмов, предотвращающих несанкционированный доступ к образам виртуальных машин, из-за ошибок его обновления.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или её части, если используется более одного гипервизора) от работоспособности гипервизора. Реализация данной угрозы возможна при условии возникновения ошибок в процессе обновления гипервизора: сбоев в процессе его обновления; обновлений, в ходе которых внедряются новые ошибки в код гипервизора; обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; других инцидентов безопасности информации						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.109.	**Угроза перебора всех настроек и параметров приложения** Угроза заключается в возможности получения нарушителем доступа к дополнительному скрытому функционалу (информация о котором не была опубликована разработчиком) или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации программы, достигая таких значений параметров путём перебора всех возможных комбинаций. Данная угроза обусловлена уязвимостями программного обеспечения, проявляющимися при его неправильной конфигурации. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на изменение конфигурации программного обеспечения. При реализации данной угрозы, в отличии от других подобных угроз, нарушитель действует «вслепую» – простым путём перебора всевозможных комбинаций						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО, микропрограммное обеспечение, реестр	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.110.	**Угроза перегрузки грид-системы вычислительными заданиями** Угроза заключается в возможности снижения пропускной способность ресурсных центров при отправке большого количества заданий одним пользователем (нарушителем) случайно или намеренно, что может сделать невозможной постановку заданий другими пользователями грид-системы в очередь на выполнение. Данная угроза обусловлена слабостями мер по контролю в грид-системе за количеством вычислительных заданий, запускаемых пользователями грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя прав на постановку заданий в очередь на выполнение грид-системой						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.111.	**Угроза передачи данных по скрытым каналам** Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы путём её нестандартного (незаметного, скрытого) размещения в легитимно передаваемых по сети (или сохраняемых на отчуждаемые носители) открытых данных путём её маскирования под служебные протоколы, сокрытия в потоке других данных (стеганография) и т.п. Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при условии наличия у нарушителя прав в дискредитируемой системе: установки специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации; доступа к каналам передачи данных						
	Отсутствует	Сетевое ПО, сетевой трафик	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.112.	**Угроза передачи запрещённых команд на оборудование с числовым программным управлением** Угроза заключается в возможности повреждения нарушителем исполнительных механизмов, заготовки и (или) обрабатывающего инструмента оборудования с числовым программным управлением путём передачи на него команд, приводящих к перемещению обрабатывающего инструмента за допустимые пределы (т.е. команд, запрещённых для оборудования с числовым программным управлением). Данная угроза обусловлена слабостями мер по защите оборудования с числовым программным управлением от выполнения запрещённых команд. Реализация данной угрозы возможна при наличии у нарушителя привилегий на передачу команд на оборудование с числовым программным управлением или возможности изменения команд, передаваемых легальным пользователем						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.113.	**Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники** Угроза заключается в возможности сброса пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Данная угроза обусловлена свойством оперативной памяти обнулять своё состояние при выключении и перезагрузке. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо) при выполнении следующих условий:						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	наличие в системе открытых сессий работы пользователей; наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, аппаратное обеспечение	Средний	Высокая	Средний	**Актуальна**	
У.114.	**Угроза переполнения целочисленных переменных** Угроза заключается в возможности приведения нарушителем дискредитируемого приложения к сбоям в работе путём подачи на его входные интерфейсы данных неподдерживаемого формата или выполнения с его помощью операции, в результате которой будут получены данные неподдерживаемого дискредитируемым приложением формата. Данная угроза обусловлена уязвимостями программного обеспечения, связанными с недостаточной проверкой такими приложениями корректности входных данных, а также тем, что операторы любого программного обеспечения способны правильно обрабатывать только определённые типы данных (например, только целые или только положительные числа). Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о номенклатуре поддерживаемых дискредитируемым приложением форматов входных (или обрабатываемых) данных; возможности взаимодействия с входным интерфейсом дискредитируемого приложения						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.115.	**Угроза перехвата вводимой и выводимой на периферийные устройства информации** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информации, вводимой и выводимой на периферийные устройства, путём перехвата данных, обрабатываемых контроллерами периферийных устройств. Данная угроза обусловлена недостаточностью мер защиты информации от утечки и контроля потоков данных, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью криптографических средств (т.к. представление пользователям системы информации должно осуществляться в доступном для понимания виде). Реализация данной угрозы возможна при условии наличия у нарушителя привилегий на установку и запуск специализированных вредоносных программ, реализующих функции «клавиатурных шпионов» (для получения нарушителем паролей пользователей), виртуальных драйверов принтеров (перехват документов, содержащих защищаемую информацию) и др.						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, прикладное ПО, аппаратное обеспечение	Средний	Высокая	Средний	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.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 данных						
	Внешний нарушитель с низким потенциалом (N1)	Сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.117.	**Угроза перехвата привилегированного потока** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к потоку данных, созданного приложением с дополнительными привилегиями (к привилегированному потоку данных), путём синхронного (вызов привилегированной функции, возвращающей неправильное значение) или асинхронного (создание обратных вызовов, манипулирование указателями и т.п.) деструктивного программного воздействия на него. Данная угроза обусловлена уязвимостями программного обеспечения, использующего в своей работе участки кода, исполняемого с дополнительными правами, наследуемыми создаваемыми привилегированными потоками (наличие ошибочных указателей, некорректное освобождение памяти и т.п.). Реализация данной угрозы возможна в следующих условиях: в дискредитируемом приложении существуют участки кода, требующие исполнения с правами, превышающими права обычных пользователей; нарушитель обладает привилегиями, позволяющими вносить изменения во входные данные дискредитируемого приложения						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.118.	**Угроза перехвата привилегированного процесса** Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя или группы пользователей, выполняющих роль администраторов дискредитируемой системы), для выполнения произвольного вредоносного кода с правами дискредитированного процесса. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации), приводящими к некорректному распределению прав доступа внутри древа наследуемых процессов.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при выполнении одного из условий: успешного введения нарушителем некорректных данных, приводящих к переполнению буфера или к реализации некоторых типов программных инъекций; наличия у нарушителя привилегий на запуск системных утилит, предназначенных для управления процессами						
	Отсутствует	Системное ПО, прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.119.	**Угроза перехвата управления гипервизором** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым гипервизором, за счёт получения нарушителем права управления гипервизором путём эксплуатации уязвимостей консоли управления гипервизором. Данная угроза обусловлена наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью управления гипервизором						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.120.	**Угроза перехвата управления средой виртуализации** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам, зарезервированным и управляемым всеми гипервизорами, реализующими среду виртуализации, за счёт получения нарушителем права управления этими гипервизорами путём эксплуатации уязвимостей консоли средства управления виртуальной инфраструктурой. Данная угроза обусловлена наличием у консоли средства управления виртуальной инфраструктурой, реализуемого в рамках одной из виртуальных машин, программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данной консоли (программа уровня управления виртуализации), а также недостаточностью мер по разграничению доступа к данной консоли. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с консолью средства управления виртуальной инфраструктурой						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							Данная технология не применяется в ИС
У.121.	**Угроза повреждения системного реестра** Угроза заключается в возможности нарушения доступности части функционала или всей информационной системы из-за повреждения используемого в её работе реестра вследствие некорректного завершения работы операционной системы (неконтролируемая перезагрузка, возникновения ошибок в работе драйверов устройств и т.п.), нарушения целостности файлов, содержащих в себе данные реестра, возникновения ошибок файловой системы носителя информации или вследствие осуществления нарушителем деструктивного программного воздействия на файловые объекты, содержащие реестр. Данная угроза обусловлена слабостями мер контроля доступа к файлам, содержащим данные реестра, мер резервирования и контроля целостности таких файлов, а также мер восстановления работоспособности реестра из-за сбоев в работе операционной системы. Реализация данной угрозы возможна при одном из условий: возникновения ошибок в работе отдельных процессов или всей операционной системы; наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра						
	Внешний нарушитель с низким потенциалом (N1)	Объекты файловой системы, реестр	Средний	Высокая	Средний	**Актуальна**	
У.122.	**Угроза повышения привилегий** Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемый процесс (или систему) или на другие процессы (или системы) от его (её) имени путём эксплуатации неправомерно полученных нарушителем дополнительных прав на управление дискредитированным объектом. Данная угроза обусловлена уязвимостями программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации). Реализация данной угрозы возможна при наличии у нарушителя программного обеспечения (типа «эксплойт»), специально разработанного для реализации данной угрозы в дискредитируемой системе						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, сетевое ПО, информационная система	Средний	Высокая	Средний	**Актуальна**	
У.123.	**Угроза подбора пароля BIOS** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI путём входа в консоль BIOS/UEFI по паролю, подобранному программно или «вручную» с помощью методов тотального перебора вариантов или подбора по словарю. Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев:						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	нарушитель может осуществить физический доступ к компьютеру и имеет возможность его перезагрузить; нарушитель обладает специальным программным средством перебора паролей BIOS/UEFI и привилегиями в системе на установку и запуск таких средств						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.124.	**Угроза подделки записей журнала регистрации событий** Угроза заключается в возможности внесения нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о не произошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз. Данная угроза обусловлена недостаточностью мер по разграничению доступа к журналу регистрации событий безопасности. Реализация данной угрозы возможна в одном из следующих случаев: технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования и нарушитель обладает необходимыми для этого привилегиями; технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО	Средний	Высокая	Средний	**Актуальна**	
У.125.	**Угроза подключения к беспроводной сети в обход процедуры аутентификации** Угроза заключается в возможности осуществления нарушителем перехвата трафика беспроводной сети или других неправомерных действий путём легализации нарушителем собственного подключения к беспроводной сети в полуавтоматическом режиме (например, WPS) без ввода ключа шифрования. Данная угроза обусловлена слабостями процедуры аутентификации беспроводных устройств в ходе полуавтоматического подключения. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к беспроводной точке доступа, поддерживающей полуавтоматический режим подключения						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.126.	**Угроза подмены беспроводного клиента или точки доступа** Угроза заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	подключения точек беспроводного доступа или клиентского программного обеспечения к доверенным субъектам сетевого взаимодействия, подменённым нарушителем. Данная угроза обусловлена слабостями механизма аутентификации субъектов сетевого взаимодействия при беспроводном доступе. Реализация данной угрозы возможна в случае размещения нарушителем клиента или точки беспроводного доступа со специально сформированными параметрами работы (такими как MAC-адрес, название, используемый стандарт передачи данных и т.п.) в зоне доступности для дискредитируемых устройств беспроводного доступа						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.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						
	Отсутствует	Прикладное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.128.	**Угроза подмены доверенного пользователя** Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени. Данную угрозу можно охарактеризовать как «имитация действий клиента». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника/получателя информации. Реализация данной угрозы возможна при наличии у нарушителя подключения к вычислительной сети, а также сведений о конфигурации сетевых устройств, типе используемого программного обеспечения и т.п.						
	Внешний нарушитель с низким потенциалом (N1)	СетевоеПО	Средний	Высокая	Средний	**Актуальна**	
У.129.	**Угроза подмены резервной копии программного обеспечения BIOS** Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	или создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения BIOS/UEFI, предварительно подменённой нарушителем. Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в следующих условиях: нарушитель успешно подменил резервную копию программного обеспечения BIOS/UEFI; возникла необходимость восстановления предыдущей версии программного обеспечения BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.130.	**Угроза подмены содержимого сетевых ресурсов** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены содержимого хранящихся (сайты, веб-страницы) или передаваемых (электронные письма, сетевые пакеты) по сети данных. Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности содержимого электронного сообщения. Реализация данной угрозы возможна при условии наличия у нарушителя прав на доступ к сетевым ресурсам и отсутствии у пользователя сети мер по обеспечению их целостности						
	Внешний нарушитель с низким потенциалом (N1)	Прикладное ПО, сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.131.	**Угроза подмены субъекта сетевого доступа** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения. Данную угрозу можно охарактеризовать как «имитация действий сервера». Данная угроза обусловлена слабостями технологий сетевого взаимодействия, зачастую не позволяющими выполнить проверку подлинности источника информации. Реализация данной угрозы возможна при условии успешной выдачи себя нарушителем за законного отправителя (например, с помощью ложных фишинговых веб-сайтов). Ключевое отличие от «угрозы подмены содержимого сетевых ресурсов» заключается в том, что в данном случае нарушитель не изменяет оригинального содержимого электронного ресурса (веб-сайта, электронного письма), а только служебные сведения						
	Отсутствует	Прикладное ПО, сетевое ПО,	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
		сетевой трафик					осуществить угрозу
У.132.	**Угроза получения предварительной информации об объекте защиты** Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и др., путём проведения мероприятий по сбору и анализу доступной информации о системе. Данная угроза обусловлена наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). Реализация данной угрозы возможна при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы: анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию (о трассировке стека, о конфигурации системы, о маршруте прохождения сетевых пакетов) анализ реакций системы на строковые URI-запросы (в т.ч. неверные SQL-запросы, альтернативные пути доступа к файлам). Данная угроза отличается от угрозы перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает					
	Отсутствует	Сетевой узел, сетевое ПО, сетевой трафик, прикладное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.133.	**Угроза получения сведений о владельце беспроводного устройства** Угроза заключается в возможности раскрытия нарушителем сведений о географических перемещениях дискредитируемого пользователя в определённые промежутки времени, в том числе выявить место его работы, проживания и т.п. Получение таких сведений может использоваться нарушителем в дальнейшем для реализации угроз в информационных системах, доступ к которым имеет дискредитируемый пользователь. Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет. Реализация данной угрозы возможна при условии наличия у нарушителя доступа к идентификационными данным стационарных точек беспроводного доступа, с которыми в автоматическом режиме осуществляет взаимодействие беспроводное устройство дискредитируемого пользователя					
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.134.	**Угроза потери доверия к поставщику облачных услуг** Угроза заключается в возможности снижения уровня защищённости и допущения дополнительных ошибок в обеспечении безопасности защищаемой в облачной системе информации из-за невосполнимого оттока у поставщика облачных услуг необходимых ресурсов в связи с потерей потребителями облачных услуг доверия к их поставщику.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена тем, что из-за обнародования фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, происходит потеря доверия к такому поставщику со стороны потребителей облачных услуг, и, как следствие, возникает необходимость лавинообразного выделения поставщиком облачных услуг ресурсов (человеческих, технических, финансовых) для решения возникающих в данной ситуации задач (множественные консультации пользователей, экстренный пересмотр политик безопасности, модернизация системы защиты и др.), что не только может вызвать нехватку ресурсов для обеспечения текущего уровня защищённости информации, но и спровоцировать допуск «в спешке» новых ошибок. Реализация данной угрозы возможна в случае обнародования единичных или множественных фактов об инцидентах информационной безопасности, связанных с поставщиком облачных услуг, повлёкших значительные убытки для его клиентов						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.135.	**Угроза потери и утечки данных, обрабатываемых в облаке** Угроза заключается в возможности нарушения конфиденциальности, целостности и доступности защищаемой информации потребителей облачных услуг, обрабатываемой в облачной системе. Данная угроза обусловлена слабостями мер защиты информации, обрабатываемой в облачной системе. Реализация данной угрозы возможна в случае допущения поставщиком (некорректный выбор или настройка средств защиты) или потребителем (потеря пароля, электронного ключа, вход с небезопасной консоли) облачных услуг ошибок при обеспечении безопасности защищаемой информации						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.136.	**Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных** Угроза заключается в возможности допуска ошибок при копировании защищаемой информации при распределённом хранении данных на различных узлах хранилища больших данных вследствие несогласованности их работы, влекущих за собой невозможность осуществления легальным пользователем доступа к блокам или ко всей защищаемой информации. Данная угроза обусловлена слабостями механизмов репликации данных, реализованных в узлах хранилища больших данных. Реализация данной угрозы возможна в условиях отключения или выведения из строя одного или нескольких узлов за счёт специальных программных воздействий на узлы хранилища больших данных, а также возникновения технических или программных сбоев в работе их компонентов						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.137.	**Угроза потери управления облачными ресурсами** Угроза заключается в возможности нарушения договорных обязательств со стороны поставщика облачных услуг в отношении их потребителя из-за значительной сложности построения эффективной системы управления облачными ресурсами облачной системы, особенно использующей облачные ресурсы других поставщиков облачных услуг. Данная угроза обусловлена сложностью определения логического и физического местоположения облачных ресурсов, недостаточностью мер физического контроля доступа к хранилищам данных, резервного копирования и др., а также необходимостью учёта особенностей законодательства в области защиты информации стран, резидентами которых являются поставщики облачных услуг, выполняющих роль субподрядчиков по оказанию заказанных облачных услуг. Реализация данной угрозы возможна при условии, что выполнение требований к функционалу облачной системы затрудняется (или становится невозможным) из-за правовых норм других стран, участвующих в трансграничной передаче облачного трафика						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.138.	**Угроза потери управления собственной инфраструктурой при переносе её в облако** Угроза заключается в возможности допуска ошибок в управлении инфраструктурой системы потребителя облачных услуг, иммигрированной в облако, со стороны поставщика облачных услуг из-за отсутствия у него сведений об особенностях управления конкретной системы, а также из-за отсутствия у потребителя облачных услуг, обладающего такими сведениями, возможности проводить весь комплекс работ по управлению инфраструктурой собственной системы в связи с её иммиграцией в облако. Данная угроза обусловлена невозможностью достоверной оценки потребителем облачных услуг реального уровня защищённости, обеспечиваемого поставщиком облачных услуг в отношении защищаемой информации потребителя облачных услуг, в связи с закрытостью для потребителей сведений о применяемых поставщиком облачных услуг технологиях, программных и технических решениях, а также конкретных параметрах настроек средств защиты информации. Реализация данной угрозы возможна в случаях передачи поставщику облачных услуг части функций управления системой потребителя облачных услуг (при миграции части или всей системы в облако)						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.139.	**Угроза преодоления физической защиты** Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.)						
	Внешний нарушитель снизким потенциалом (N1)	Сервер, носитель информации, аппаратное обеспечение	Средний	Средняя	Средний	**Актуальна**	
У.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 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						
	Внешний нарушитель с низким потенциалом (N1)	Информационная система, системное ПО, сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.141.	**Угроза привязки к поставщику облачных услуг** Угроза заключается в возможности возникновения трудно решаемых (или даже неразрешимых) проблем технического, организационного, юридического или другого характера, препятствующих осуществлению потребителем облачных услуг смены их поставщика. Данная угроза обусловлена отсутствием совместимости между форматами данных и программными интерфейсами, используемыми в облачных инфраструктурах различных поставщиков облачных услуг. Реализация данной угрозы возможна при условии использования поставщиком облачных услуг нестандартного программного обеспечения или формата образов виртуальных машин и отсутствием средств преобразования образа виртуальной машины из используемого им формата в другой (используемый другим поставщиком)						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.142.	**Угроза приостановки оказания облачных услуг вследствие технических сбоев** Угроза заключается в возможности снижения качества облачных услуг (или даже отказа в их оказании конечным потребителям) из-за возникновения технических сбоев хотя бы у одного из поставщиков облачных услуг (входящих в цепь посредников при оказании облачных услуг их конечному потребителю), а также из-за возникновения существенных задержек или потерь в каналах передачи данных, арендуемых потребителем или поставщиками облачных услуг. Данная угроза обусловлена слабостями процедуры контроля за выполнением технического обслуживания и соблюдением режимов функционирования технических средств облачной информационной системы. Реализация данной угрозы возможна при условии отсутствия механизмов резервирования средств обработки, хранения и передачи информации, входящих в состав облачной информационной системы						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.143.	**Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации** Угроза заключается в возможности прерывания нарушителем технологии обработки информации в дискредитируемой системе путём осуществления деструктивного программного (локально или удалённо) воздействия на средства хранения (внешних, съёмных и внутренних накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных данных на средства хранения, обработки и (или) ввода/вывода/передачи информации						
	Отсутствует	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.144.	**Угроза программного сброса пароля BIOS** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	путём ввода «пустого» пароля. Данная угроза обусловлена слабостями мер разграничения доступа в операционной системе к функции сброса пароля BIOS/UEFI. Реализация данной угрозы возможна при условиях: наличия в программном обеспечении BIOS/UEFI активного интерфейса функции программного сброса пароля непосредственно из-под операционной системы; наличия у нарушителя специальных программных средств, реализующих сброс пароля, а также прав в операционной системе для установки и запуска данных средств						
	Отсутствует	Микропрограммное обеспечение BIOS/UEFI, системное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.145.	**Угроза пропуска проверки целостности программного обеспечения** Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Данная угроза обусловлена слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения. Реализация данной угрозы возможна при условии успешного использования обманных техник одного из следующих методов: «ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, прикладное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.146.	**Угроза прямого обращения к памяти вычислительного поля суперкомпьютера** Угроза заключается в возможности осуществления процессом нарушителя, функционирующем в вычислительном поле суперкомпьютера, считывания защищаемых данных из оперативной памяти, выделенной для параллельного (дискредитируемого) процесса, с использованием операций удалённого прямого доступа к памяти. Данная угроза обусловлена слабостями протокола прямого доступа к оперативной памяти, с помощью которого выполняется обращение к сегменту памяти, выделенному для удалённого параллельного процесса, функционирующего в вычислительном поле суперкомпьютера. Реализация данной угрозы возможна при условии успешного осуществления нарушителем доступа к входным/выходным данным параллельных процессов в вычислительном поле суперкомпьютера						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.147.	**Угроза распространения несанкционированно повышенных прав на всю грид-систему** Угроза заключается в возможности автоматического распространения на всю грид-систему несанкционированно полученных нарушителем на одном узле привилегий. Данная угроза обусловлена наличием уязвимостей в клиентском программном обеспечении грид-системы и слабостями в механизме назначения прав пользователям, реализованном в связующем программном обеспечении. Реализация данной угрозы возможна при условии успешного повышения нарушителем своих прав на одном узле грид-системы						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.148.	**Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных** Угроза заключается в возможности возникновения ситуаций, связанных с ошибками автоматического назначения пользователям прав доступа (наделение дополнительными полномочиями, ошибочное наследование, случайное восстановление «неактивных» учётных записей т.п.). Данная угроза обусловлена слабостями мер контроля за большим количеством (от тысячи, а в некоторых случаях и до нескольких миллионов) учётных записей пользователей со стороны администраторов безопасности. Реализация данной угрозы возможна при условии возникновения сбоев или ошибок в работе системы разграничения доступа хранилища больших данных						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.149.	**Угроза сбоя обработки специальным образом изменённых файлов** Угроза заключается в возможности осуществления нарушителем различных неправомерных действий от имени дискредитированных приложений путём вызова сбоя в их работе за счёт внесения изменений в обрабатываемые дискредитируемыми программами файлы или их метаданные. Данная угроза обусловлена слабостями механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна в условиях: наличия у нарушителя сведений о форматах и значениях файлов, вызывающих сбой функционирования дискредитированных приложений при их обработке; успешно созданном в дискредитируемой системе механизме перехвата управления над обработкой нарушителем программного сбоя						
	Отсутствует	Метаданные, объекты файловой системы, системное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.150.	**Угроза сбоя процесса обновления BIOS** Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение BIOS/UEFI в результате нарушения процесса его обновления. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии обновления (из-за сбоев, помех и т.п.), так и при установке повреждённой/несовместимой версии обновления (из-за отсутствия механизма проверки целостности и совместимости)						
	Отсутствует	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.151.	**Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL** Угроза заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера. Данная угроза обусловлена недостаточностью мер по обеспечению конфиденциальности информации, реализованных в WSDL-сервисах, предоставляющих подробные сведения о портах, службах и соединениях, доступных пользователям. Реализация данной угрозы возможна при наличии у нарушителя сетевого доступа к исследуемому сетевому ресурсу и специальных программных средств сканирования сети						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.152.	**Угроза удаления аутентификационной информации** Угроза заключается в возможности отказа легитимным пользователям в доступе к информационным ресурсам, а также в возможности получения нарушителем привилегий дискредитированного пользователя за счёт сброса (обнуления, удаления) его аутентификационной информации. Данная угроза обусловлена слабостями политики разграничения доступа к аутентификационной информации и средствам работы с учётными записями						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	пользователей. Реализация данной угрозы возможна при выполнении одного из следующих условий: штатные средства работы с учётными записями пользователей обладают функционалом сброса аутентификационной информации, и нарушитель получил привилегии в дискредитируемой системе на использование данных средств; нарушитель обладает специальным программным обеспечением, реализующим функцию сброса аутентификационной информации, и получил привилегии в дискредитируемой системе на использование данных средств						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, микропрограммное обеспечение, учётные данные пользователя	Средний	Высокая	Средний	**Актуальна**	
У.153.	**Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов** Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объёмом сетевого трафика, генерируемого сторонними серверами в ответ на сетевые запросы нарушителя, сформированные от имени дискредитируемой системы. Генерируемый сторонними серверами сетевой трафик значительно превышает объём сетевых запросов, формируемых нарушителем. Данная угроза обусловлена слабостями мер межсетевого экранирования дискредитируемой информационной системы, мер контроля подлинности сетевых запросов на сторонних серверах, а также слабостями модели взаимодействия открытых систем. Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о сторонних серверах с недостаточными мерами контроля подлинности сетевых запросов; сведений о сетевом адресе дискредитируемой системы; специального программного обеспечения, реализующего функции генерации сетевых пакетов						
	Внешний нарушитель с низким потенциалом (N1)	Информационная система, системное ПО, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.154.	**Угроза установки уязвимых версий обновления программного обеспечения BIOS** Угроза заключается в возможности внесения уязвимостей в программное обеспечение BIOS/UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации BIOS/UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера						
	Отсутствует	Микропрограммное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
		BIOS/UEFI					осуществить угрозу
У.155.	**Угроза утраты вычислительных ресурсов** Угроза заключается в возможности отказа легитимному пользователю в выделении ресурсов для обработки его запросов из-за исчерпания нарушителем свободных ресурсов в системе, осуществлённого путём их несанкционированного исключения из общего пула ресурсов на основе техник «утечки ресурсов» или «выделения ресурсов». Данная угроза обусловлена слабостями механизма контроля за распределением вычислительных ресурсов между пользователями, а также мер межсетевого экранирования дискредитируемой информационной системы и контроля подлинности сетевых запросов на сторонних серверах. Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о формате и параметрах деструктивных воздействий на систему, приводящих к исключению («утечки» или «выделению») свободных ресурсов из общего пула ресурсов дискредитируемой системы; привилегий, достаточных для осуществления деструктивных воздействий («утечки» или «выделения») в дискредитируемой системе; отсутствие у администраторов возможности: для техники «утечки ресурсов» – перезагрузки системы во время отправки нарушителем большого числа запросов на выделение ресурсов, а для техники «выделения ресурсов» – форсированного освобождения ресурсов, выделенных по запросам вредоносных процессов						
	Внешний нарушитель с низким потенциалом (N1)	Информационная система, сетевой узел, носитель информации, системное ПО, сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.156.	**Угроза утраты носителей информации** Угроза заключается в возможности раскрытия информации, хранящейся на утерянном носителе (в случае отсутствия шифрования данных), или её потери (в случае отсутствия резервной копий данных). Данная угроза обусловлена слабостями мер регистрации и учёта носителей информации, а также мер резервирования защищаемых данных. Реализация данной угрозы возможна вследствие халатности сотрудников						
	Отсутствует	Носитель информации	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.157.	**Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации** Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Внешний нарушитель с низким потенциалом (N1)	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Средний	Средняя	Средний	**Актуальна**	
У.158.	**Угроза форматирования носителей информации** Угроза заключается в возможности утраты хранящейся на форматируемом носителе информации, зачастую без возможности её восстановления, из-за преднамеренного или случайного выполнения процедуры форматирования носителя информации. Данная угроза обусловлена слабостью мер ограничения доступа к системной функции форматирования носителей информации. На реализацию данной угрозы влияют такие факторы как: время, прошедшее после форматирования; тип носителя информации; тип файловой системы носителя; интенсивность взаимодействия с носителем после форматирования и др.						
	Внешний нарушитель с низким потенциалом (N1)	Носитель информации	Средний	Высокая	Средний	**Актуальна**	
У.159.	**Угроза «форсированного веб-браузинга»** Угроза заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений. Данная угроза обусловлена слабостями (или отсутствием) механизма проверки корректности вводимых данных на веб-серверах. Реализация данной угрозы возможна при условии успешной реализации «ручного ввода» в адресную строку веб-браузера определённых адресов веб-страниц и осуществления принудительного перехода по древу веб-сайта к страницам, ссылки на которые явно не указаны на веб-сайте						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.160.	**Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации** Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Внешний нарушитель с низким потенциалом (N1)	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	Средний	Высокая	Средний	**Актуальна**	
У.161.	**Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями** Угроза заключается в возможности возникновения ситуации типа «отказ в обслуживании» со стороны вычислительного поля суперкомпьютера. Данная угроза обусловлена слабостями мер контроля за распределением вычислительных ресурсов суперкомпьютера при обработке задачи несколькими процессорами Реализация данной угрозы возможна при условии выполнения суперкомпьютером специфичных вычислительных задач, в ходе которых генерируются межпроцессорные сообщения с большой интенсивностью						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.162.	**Угроза эксплуатации цифровой подписи программного кода** Угроза заключается в возможности повышения нарушителем привилегий в системах, использующих цифровую подпись кода в качестве связующей информации между программой и её привилегиями, путём дискредитации механизма подписывания программного кода. Данная угроза обусловлена слабостями в механизме подписывания программного кода. Реализация данной угрозы возможна при следующих условиях: дискредитируемый программный код написан с помощью фреймворка (framework), поддерживающего подписывание программного кода; дискредитируемый программный код подписан вендором (поставщиком программного обеспечения); нарушитель имеет возможность внедрить программный код в дискредитируемый компьютер						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО, прикладное ПО	Средний	Высокая	Средний	**Актуальна**	
У.163.	**Угроза перехвата исключения/сигнала из привилегированного блока функций** Угроза заключается в возможности нарушителя получить права на доступ к защищаемой информации путём перехвата исключений/сигналов, сгенерированных участком программного кода, исполняемого с повышенными привилегиями (привилегированным блоком функций) и содержащего команды по управлению защищаемой информацией. Данная угроза обусловлена тем, что вызов программных функций в привилегированном режиме подразумевает отключение для них механизмов разграничения						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	доступа. Реализация данной угрозы возможна при следующих условиях: дискредитируемая программа, написана на языке программирования, поддерживающего механизм привилегированных блоков (например, Java); в дискредитируемой программе вызов привилегированных блоков осуществлён небезопасным способом (использовано публичное объявление внутренних функций, использована генерация исключений из привилегированного блока); нарушитель обладает правами, достаточными для перехвата программных исключений в системе						
	Отсутствует	Системное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.164.	**Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре** Угроза заключается в возможности распространения негативных последствий от реализации угроз на физическом или виртуальном уровне облачной инфраструктуры на уровни управления и оркестровки, а также на все информационные системы, развёрнутые на базе дискредитированной облачной инфраструктуры. Данная угроза обусловлена невозможностью функционирования информационных систем в облаке при некорректной работе самой облачной инфраструктуры, а также зависимостью работоспособности верхних уровней облачной инфраструктуры от работоспособности нижних. Реализация данной угрозы возможна в случае приведения облачной инфраструктуры на физическом или виртуальном уровне облачной инфраструктуры в состояние «отказ в обслуживании»						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.165.	**Угроза включения в проект не достоверно 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, разрекламированности и др.						
	Отсутствует	ПО, техническое средство, информационная система	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.166.	**Угроза внедрения системной избыточности** Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом)						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	из-за внедрения в него (в неё) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. Реализация данной угрозы возможна при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой)						
	Отсутствует	ПО, информационная система	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.167.	**Угроза заражения компьютера при посещении неблагонадёжных сайтов** Угроза заключается в возможности нарушения безопасности защищаемой информации вредоносными программами, скрытно устанавливаемыми при посещении пользователями системы с рабочих мест (намеренно или при случайном перенаправлении) сайтов с неблагонадёжным содержимым и запускаемыми с привилегиями дискредитированных пользователей. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым						
	Отсутствует	Сетевой узел, сетевое ПО	Средний	-	-	**Неактуальна**	
У.168.	**Угроза «кражи» учётной записи доступа к сетевым сервисам** Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путём получения информации идентификации/аутентификации, соответствующей учётной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты. Данная угроза обусловлена недостаточностью мер контроля за активностью/существованием ящиков электронной почты. Реализация данной угрозы возможна при условиях: наличия статуса «свободен для занимания» у адреса электронной почты, с которым связана учётная запись доступа пользователя к сетевым сервисам (например, если пользователь указал при регистрации несуществующий адрес или долго не обращался к почтовому ящику, вследствие чего, его отключили); наличия у нарушителя сведений об адресе электронной почты, с которым связана учётная запись дискредитируемого пользователя для доступа к сетевым сервисам						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.169.	**Угроза наличия механизмов разработчика** Угроза заключается в возможности перехвата управления программой за счёт использования отладочных механизмов (специальных программных функций или аппаратных элементов, помогающих проводить тестирование и отладку средств во время их разработки).						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена недостаточностью мер по контролю за ошибками в ходе разработки средств защиты информации. Реализация данной угрозы возможна при условии, что в программе не удалены отладочные механизмы						
	Отсутствует	ПО, техническое средство	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.170.	**Угроза неправомерного шифрования информации** Угроза заключается в возможности фактической потери доступности защищаемых данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа. Данная угроза обусловлена наличием слабостей в антивирусной защите, а также в механизмах разграничения доступа. Реализация данной угрозы возможна при условии успешной установки нарушителем на дискредитируемый компьютер средства криптографического преобразования информации, а также успешного обнаружения (идентификации) нарушителем защищаемых файлов						
	Внешний нарушитель с низким потенциалом (N1)	Объект файловой системы	Средний	Высокая	Средняя	**Актуальна**	
У.171.	**Угроза скрытного включения вычислительного устройства в состав бот-сети** Угроза заключается в возможности опосредованного осуществления нарушителем деструктивного воздействия на информационные системы с множества вычислительных устройств (компьютеров, мобильных технических средств и др.), подключённых к сети Интернет, за счёт захвата управления такими устройствам путём несанкционированной установки на них: вредоносного ПО типа Backdoor для обеспечения нарушителя возможностью удалённого доступа/управления дискредитируемым вычислительным устройством; клиентского ПО для включения в ботнет и использования созданного таким образом ботнета в различных противоправных целях (рассылка спама, проведение атак типа «отказ в обслуживании» и др.). Данная угроза обусловлена уязвимостями в сетевом программном обеспечении и слабостями механизмов антивирусного контроля и межсетевого экранирования. Реализация данной угрозы возможна при условии наличия выхода с дискредитируемого вычислительного устройства в сеть Интернет						
	Внешний нарушитель с низким потенциалом (N1)	Сетевой узел, сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.172.	**Угроза распространения «почтовых червей»** Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем, содержащих вредоносную программу типа «почтовый червь», а также невольного участия в						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	дальнейшем противоправном распространении вредоносного кода. Данная угроза обусловлена слабостями механизмов антивирусного контроля. Реализация данной угрозы возможна при условии наличия у дискредитируемого пользователя электронного почтового ящика, а также наличия в его адресной книге хотя бы одного адреса другого пользователя						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.173.	**Угроза «спама» веб-сервера** Угроза заключается в возможности неправомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов. Данная угроза обусловлена уязвимостями механизмов фильтрации сообщений, поступающих из сети Интернет. Реализация данной угрозы возможна при условии наличия в дискредитируемом веб-сервере активированного функционала, реализующего различные почтовые сервера, службы доставки мгновенных сообщений, блоги, форумы, аукционы веб-магазинов, онлайн-сервисы отправки SMS-сообщений, онлайн-сервисы голосования и др.						
	Внешний нарушитель с низким потенциалом (N1)	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС
У.174.	**Угроза «фарминга»** Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём скрытного перенаправления пользователя на поддельный сайт (выглядящий одинаково с оригинальным), на котором от дискредитируемого пользователя требуется ввести защищаемую информацию. Данная угроза обусловлена уязвимостями DNS-сервера, маршрутизатора. Реализация данной угрозы возможна при условии наличия у нарушителя: сведений о конкретных сайтах, посещаемых пользователем, на которых требуется ввод защищаемой информации; средств создания и запуска поддельного сайта; специальных программных средств типа «эксплойт», реализующих перенаправление пользователя на поддельный сайт. Кроме того, угрозе данного типа подвержены подлинные сайты, не требующие установления безопасного соединения перед вводом информации ограниченного доступа						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.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-phishingattack), с помощью звонков с вопросом об открытии вложения письма, имитацией рекламных предложений (fakeoffers) или различных приложений (fakeapps)) зайти на поддельный сайт (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)						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО, сетевой трафик	Средний	Высокая	Средний	**Актуальна**	
У.176.	**Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты** Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации средствами защиты информации, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации угроз безопасности информации. На реализацию данной угрозы влияет не только номенклатура применяемых средств защиты информации, параметры их настройки, объём передаваемой/обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации						
	Внешний нарушитель с низким потенциалом (N1)	Средство защиты информации	Средний	Высокая	Средний	**Актуальна**	
У.177.	**Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью** Угроза заключается в возможности возникновения ошибок в работе системы вследствие отсутствия (или игнорирования) процедуры обнаружения и исправления ошибок в данных, вводимых во время работы самим оператором, до активизации управляемого оборудования. Кроме того, к реализации данной угрозы могут привести некорректно реализованные (или отсутствующие) средства реагирования на неправильные, самопроизвольные действия оператора, средства учёта нижних/верхних пределов скорости и направления реакции оператора, схемы реагирования на двойное нажатие клавиш при вводе обычных и критических данных, процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.).						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализуемость данной угрозы зависит от требований, предъявляемых к процедурам обнаружения и исправления ошибок во вводимых данных в систему, связанную с безопасностью, а также разницей между этими требованиями и фактическим уровнем обнаружения и исправления ошибок						
	Отсутствует	Системное ПО, сетевое ПО, прикладное ПО, аппаратное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.178.	**Угроза несанкционированного использования системных и сетевых утилит** Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на систему за счёт использования имеющихся или предварительно внедрённых стандартных (известных и обычно не определяемых антивирусными программами как вредоносных) системных и сетевых утилит, предназначенных для использования администратором для диагностики и обслуживания системы (сети). Реализация данной угрозы возможна при условиях: наличие в системе стандартных системных и сетевых утилит или успешное их внедрение нарушителем в систему и сокрытие (с использованием существующих архивов, атрибутов «скрытый» или «только для чтения» и др.); наличие у нарушителя привилегий на запуск таких утилит						
	Внешний нарушитель с низким потенциалом (N1)	Системное ПО	Средний	Высокая	Средний	**Актуальна**	
У.179.	**Угроза несанкционированной модификации защищаемой информации** Угроза заключается в возможности нарушения целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём. Реализация данной угрозы возможна в случае получения нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия						
	Внешний нарушитель с низким потенциалом (N1)	Объекты файловой системы	Средний	Высокая	Средний	**Актуальна**	
У.180.	**Угроза отказа подсистемы обеспечения температурного режима** Угроза заключается в возможности повреждения части компонентов системы или системы в целом вследствие выхода температурного режима их работы из заданных требований из-за возникновения отказа входящих в неё подсистем вентиляции и температурных приборов. Реализация данной угрозы возможна как вследствие естественных техногенных причин, так и путём проведения определённых мероприятий нарушителем,						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима						
	Внешний нарушитель с низким потенциалом (N1)	Технические средства воздушного кондиционирования	Средний	Высокая	Средний	**Актуальна**	
У.181.	**Угроза перехвата одноразовых паролей в режиме реального времени** Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путём перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечёт их срок действия (обычно, не более 5 минут). Реализация данной угрозы возможна при выполнении следующих условий: наличие у нарушителя сведений об информации идентификации/аутентификации дискредитируемого пользователя условно-постоянного действия; успешное осуществление нарушителем перехвата трафика между системой и пользователем						
	Отсутствует	Сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.182.	**Угроза физического устаревания аппаратных компонентов** Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.), обусловленного влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций). Возможность реализации данной угрозы возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем						
	Отсутствует	Аппаратное средство	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.183.	**Угроза перехвата управления автоматизированной системой управления технологическими процессами** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных. Данная угроза обусловлена наличием у автоматизированной системы управления технологическими процессами программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами. Реализация данной угрозы может привести к: блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия; нарушению штатного хода технологических процессов; частичному или полному останову технологических процессов без (или с) выхода(-ом) оборудования из строя; аварийной ситуации в критической системе информационной инфраструктуры						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.184.	**Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства** Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); видеоданные, снимаемые видеокамерами мобильного устройства; аудиоданные, снимаемые микрофоном устройства						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.185.	**Угроза несанкционированного изменения параметров настройки средств защиты информации** Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки средства защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к конфигурационным файлам средства защиты информации. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации						
	Внешний нарушитель с низким потенциалом (N1)	Средство защиты информации	Средний	Высокая	Средний	**Актуальна**	
У.186.	**Угроза внедрения вредоносного кода через рекламу, сервисы и контент** Угроза заключается в возможности внедрения нарушителем в информационную систему вредоносного кода посредством рекламы, сервисов и (или) контента (т.е. убеждения пользователя системы активировать ссылку, код и др.) при посещении пользователем системы сайтов в сети Интернет или установкой программ с функцией показа рекламы. Данная угроза обусловлена слабостями механизмов фильтрации сетевого трафика и антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов в сети Интернет						
	Внешний нарушитель с низким потенциалом (N1)	Сетевое ПО	Средний	Высокая	Средний	**Актуальна**	
У.187.	**Угроза несанкционированного воздействия на средство защиты информации** Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к программной среде управления средством защиты информации и изменения режима его функционирования. Угроза обусловлена наличием у средств защиты информации программной среды управления и взаимодействия с пользователями системы. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации						
	Отсутствует	Средство защиты информации	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.188.	**Угроза подмены программного обеспечения** Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения.						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Данная угроза обусловлена наличием у пользователя прав для установки программного обеспечения из сети Интернет. Реализация данной угрозы возможна при скачивании программного обеспечения в сети Интернет						
	Отсутствует	Прикладное ПО, сетевое ПО, системное ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.189.	**Угроза маскирования действий вредоносного кода** Угроза заключается в возможности сокрытия в системе действий вредоносного кода за счет применения специальных механизмов маскирования кода (архивирование, изменение формата данных и др.), которые препятствуют его дальнейшему анализу. Данная угроза обусловлена наличием способов маскирования программного кода, не учтенных сигнатурными базами средств защиты информации, а также механизмов операционной системы, позволяющих осуществить поиск модулей средств защиты информации. Реализация данной угрозы возможна при условии использования в системе устаревших версий средств защиты информации						
	Отсутствует	Системное ПО, сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.190.	**Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет** Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещаемые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевого экранирования. Реализация данной угрозы возможна при: неограниченном доступе пользователя в сеть Интернет; наличии у нарушителя сведений о сайтах, посещаемых пользователем						
	Отсутствует	Сетевое ПО	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.191.	**Угроза внедрения вредоносного кода в дистрибутив программного обеспечения** Угроза заключается в возможности осуществления нарушителем заражения системы путем установки дистрибутива, в который внедрен вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты. Реализация данной угрозы возможна при: применении пользователем сторонних дистрибутивов; отсутствии антивирусной проверки перед установкой дистрибутива						
	Внешний нарушитель с низким потенциалом	Прикладное ПО, сетевое ПО,	Средний	Высокая	Средняя	**Актуальна**	

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	(N1)	системное ПО					
У.192.	**Угроза использования уязвимых версий программного обеспечения** Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путем эксплуатации уязвимостей программного обеспечения. Данная угроза обусловлена слабостями механизмов анализа программного обеспечения на наличие уязвимостей. Реализация данной угрозы возможна при отсутствии проверки перед применением программного обеспечения на наличие в нем уязвимостей						
	Внешний нарушитель с низким потенциалом (N1)	Прикладное ПО, сетевое ПО, системное ПО	Средний	Высокая	Средний	**Актуальна**	
У.193.	**Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования графика** Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная у гроза обусловлена слабостями мер защиты информации при хранении, обработке и передаче информационных ресурсов. Реализация данной угрозы возможна: при условии успешного внедрения в дискредитируемую систему указанного вредоносного программного обеспечения: при отсутствии или недостаточной реализации мер межсетевого экранирования						
	Отсутствует	Информационные ресурсы, объекты файловой системы	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.194.	**Угроза несанкционированного использования привилегированных функций мобильного устройства** Угроза заключается в возможности снятия нарушителем предустановленных производителем ограничений на конфигурирование привилегированных функций мобильного устройства. Данная угроза обусловлена наличием уязвимостей в операционных системах мобильного устройства, позволяющих получить доступ к настройкам привилегированных функций. Реализация данной угрозы возможна при получении нарушителем доступа к мобильному устройству						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.195.	**Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы**						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Угроза заключается в возможности удаленного запуска вредоносного кода за счет создания приложений, использующих обход механизмов защиты, встроенных в операционную систему. Данная угроза обусловлена ошибками в процессорах (например, ошибками в процессоре Intel поколения Haswell), позволяющими за счет создания специальных приложений осуществлять обход механизмов защиты, встроенных в операционную систему (например, механизма ASLR). Реализация данной угрозы возможна при: инициировании коллизии в таблице целевых буферов - с ее помощью можно узнать участки памяти, где находятся конкретные фрагменты кода; создании приложения, использующего эти фрагменты кода для обхода механизма защиты; запуске данного приложения в связке с эксплойтом какой-либо уязвимости самой операционной системы для создания возможности удаленного запуска вредоносного кода						
	Отсутствует	Стационарные и мобильные устройства (компьютеры и ноутбуки)	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.196.	**Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве** Угроза заключается в возможности использования вредоносной программы для контроля списка приложений, запущенных на мобильном устройстве. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносных программ (отсутствие контроля разрешенного программного обеспечения). Реализация данной угрозы возможна при условии, что вредоносная программа внедрена на мобильном устройстве и непреднамеренно запущена самим пользователем						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.197.	**Угроза хищения аутентификационной информации из временных файлов cookie** Угроза заключается в возможности хищения с использованием вредоносной программы аутентификационной информации пользователей, их счетов, хранящейся во временных файлах cookie, и передачи этой информации нарушителям через открытый RDP-порт. Данная угроза обусловлена недостаточностью мер антивирусной защиты, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена непринятием мер по стиранию остаточной информации из временных файлов (очистке временных файлов).						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт						
	Внешний нарушитель с низким потенциалом (N1)	Прикладное ПО	Средний	Высокая	Средний	**Актуальна**	
У.198.	**Угроза скрытной регистрации вредоносной программой учетных записей администраторов** Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере. Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения). Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт						
	Внешний нарушитель с низким потенциалом (N1)	Прикладное ПО	Средний	Высокая	Средний	**Актуальна**	
У.199.	**Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов** Угроза заключается в возможности управления мобильным устройством и запущенными на нем приложениями от имени легального пользователя за счет передачи этих команд через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающийся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть, не отключен) и установлена низкая чувствительность голосового идентификатора						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
У.200.	**Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов** Угроза заключается в возможности хищения данных пользователя с его мобильного устройства через виртуальных голосовых ассистентов (например, через Siri для IPhone). Данная угроза обусловлена проблемами аутентификации пользователя, в частности по Voice ID. Голосовой ассистент не может быть полностью уверен в том, что обращающейся к нему голос принадлежит владельцу устройства, поэтому для удобства пользователей и гарантии срабатывания устанавливается низкая чувствительность Voice ID. Это позволяет нарушителю использовать записанную на диктофон речь владельца мобильного устройства. Реализация данной угрозы возможна при условии, что виртуальный голосовой ассистент находится в активном состоянии (то есть не отключен) и установлена низкая чувствительность голосового идентификатора						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.201.	**Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере** Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции автоматического заполнение форм авторизации. Реализация данной угрозы обусловлена хранением в браузерах в открытом виде пользовательских данных, используемых для автозаполнения форм авторизации. Реализация данной угрозы возможна при условии, что пользователь использует браузер, в котором реализована и активирована функция автоматического заполнения форм авторизации						
	Внешний нарушитель с низким потенциалом (N1)	Прикладное ПО	Средний	Высокая	Средний	**Актуальна**	
У.202.	**Угроза несанкционированной установки приложений на мобильные устройства** Угроза заключается в возможности установки приложений на виртуальные машины мобильных устройств, работающих под управлением операционной системы Android, несанкционированно запущенных внедренной вредоносной программой. Вредоносная программа запускает виртуальную машину на мобильном устройстве, размещает (устанавливает) в этой виртуальной машине неограниченное количество приложений. Данная угроза обусловлена недостаточностью мер по контролю за запуском прикладного программного обеспечения, что позволяет выполнить неконтролируемый запуск вредоносного прикладного программного обеспечения по факту совершения пользователем различных действий в системе						

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
	(например, при попытке закрытия пользователем нежелательной рекламы). Реализация данной угрозы возможна при условии наличия на мобильном устройстве вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу Данная технология не применяется в ИС
У.203.	**Угроза утечки информации с неподключенных к сети Интернет компьютеров** Угроза заключается в возможности хищения данных с неподключенных к сети Интернет компьютеров за счет компрометации их аппаратных элементов или устройств коммутационного оборудования (например, маршрутизаторов), оснащенных LED-индикаторами, фиксации мерцания этих индикаторов и расшифровки полученных результатов. Реализация данной угрозы обусловлена тем, что существует возможность несанкционированного получения управления этими индикаторами (с помощью специальной прошивки или повышения привилегий и выполнения вредоносного кода), позволяющего передавать информацию путем ее преобразования в последовательность сигналов индикаторов компьютеров и коммутационного оборудования. Реализация данной угрозы возможна при условии, что злоумышленником получен физический доступ к компрометируемому компьютеру или коммутационному оборудованию для установки средства визуального съема сигналов LED-индикаторов						
	Отсутствует	Программное обеспечение	Средний	-	-	**Неактуальна**	Отсутствует актуальный нарушитель, способный осуществить угрозу
У.204.	**Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров** Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и управления исполнительными устройствами в программируемых логических контроллерах после ее проникновения и авторизации на данных устройствах. Реализация угрозы обусловлена возможностью вредоносной программы обнаруживать в сети программируемые логические контроллеры, проникать и функционировать в операционной системе программируемых логических контроллеров, а также недостатками механизмов аутентификации. Реализация данной угрозы возможна при условии, что существует возможность доступа к элементам автоматизированной системы управления технологическими процессами по сети Интернет						
	Отсутствует	Аппаратное устройство	Средний	-	-	**Неактуальна**	Данная технология не

ID	Источники угрозы/ нарушители	Объект воздействия	Уровень исходной защищенности	Реализуемость угрозы	Уровень опасности	Актуальность	Обоснование
							применяется в ИС
У.205.	**Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты** Угроза заключается в возможности нарушения работы компьютера и отказа в доступе к его данным за счет ошибочного блокирования средством защиты информации файлов. Реализация данной угрозы обусловлена тем, что на компьютере установлено средство защиты информации, реализующее функцию блокирования файлов						
	Внешний нарушитель с низким потенциалом (N1)	Аппаратное устройство, программное обеспечение	Средний	Высокая	Средний	**Актуальна**	
У.206.	**Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем** Угроза заключается в прекращении работы оборудования с ЧПУ, вызванном изменением геолокационной информации о данном оборудовании. Угроза обусловлена геолокационной привязкой оборудования с ЧПУ к конкретной географической координате при пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации						
	Отсутствует	Отсутствует	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС Отсутствует актуальный нарушитель, способный осуществить угрозу
У.207.	**Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)** Угроза заключается в несанкционированном получении доступа к параметрам настройки информации в оборудовании с ЧПУ посредством использования специальных «мастер-кодов» (инженерных паролей), «жестко прописанных» (не изменяемых путем конфигурирования) в программном обеспечении данного оборудования. Угроза обусловлена необходимостью проведения ремонтных работ при сбоях в ПО оборудования с ЧПУ представителями производителя						
	Внешний нарушитель с низким потенциалом (N1)	Аппаратное устройство, программное обеспечение	Средний	-	-	**Неактуальна**	Данная технология не применяется в ИС