ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "СОЛЬ-ИЛЕЦКИЙ ИНДУСТРИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ" ОРЕНБУРГСКОЙ ОБЛАСТИ

УТВЕРЖДАЮ
Директор ГАПОУ «С-ИИТТ»
_____ П.З. Малыхина
«10» августа 2023 г.

Модель угроз безопасности информации информационной системы *«Бухгалтерский и кадровый учет»*

г. Соль-Илецк
2023

Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата | Инв. № подл.

Лист согласования

Наименование организации-предприятия	Должность	ФИО	Подпись	Дата
ГАПОУ «С-ИИТТ»	Заместитель директора по АХЧ	Нуретдинов Г. Ш.		10.08.2023
ГАПОУ «С-ИИТТ»	Специалист по защите информации	Мальцев Е.А.		10.08.2023

Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата | Инв. № подл

Лит	Изм.	№ докум.	Подп.	Дата

Разраб.			
Пров.			
Т. контр.			
Н. контр.			
Утв.			

Модель угроз безопасности информации информационной системы «Зарплата и кадры»

Лит	Лист	Листов
	2	78

Содержание

Список принятых сокращений и обозначений

Сокращение или обозначение	Расшифровка
АРМ	Автоматизированное рабочее место
АСУ ТП	Автоматизированная система управления технологическим процессом
БД	База данных
БДУ	Банк данных угроз
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СКЗИ	Средства криптографической защиты информации
СУБД	Система управления базами данных
СФ	Среда функционирования
СПО	Специализированное программное обеспечение
УБИ	Угроза безопасности информации
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации

1. Общие положения

Настоящая Модель угроз разработана с целью определения актуальных угроз безопасности информации, реализация которых может привести к нарушению безопасности информации ИС «Бухгалтерский и кадровый учет».

Модель угроз содержит описание ИС «Бухгалтерский и кадровый учет» и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей, объектов воздействия, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Обладатель информации (заказчик): ГАПОУ «С-ИИТТ»

Оператор ИС «Бухгалтерский и кадровый учет»: ГАПОУ «С-ИИТТ»

2. Нормативно-правовое обеспечение разработки модели угроз

ИС «Бухгалтерский и кадровый учет» должна соответствовать следующим нормативно-правовым документам:

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

2) Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»;

3) Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

4) Приказ ФСБ от 10.07.2014 № 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».

Также при разработке настоящей Модели угроз учтены требования следующих нормативно-правовых и методических документов:

1) Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15.02.2008 заместителем директора ФСТЭК России);

2) Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru);

3) Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31.03.2015, № 149/7/2/6-432).

3. Условия уточнения модели угроз

Настоящая Модель угроз подлежит уточнению:

- по решению Оператора ИС «Бухгалтерский и кадровый учет»;
- в случае изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации;
- в случае выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;
- в случае появления сведений и фактов о новых возможностях нарушителей;
- в случае внесения изменений в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), в т.ч. включения в него сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

4. Описание информационной системы и особенностей ее функционирования

4.1. Основания использования информационной системы

Основанием для использования в ГАПОУ «С-ИИТТ» ИС «Бухгалтерский и кадровый учет» является производственная необходимость в автоматизации обработки данных работников ГАПОУ «С-ИИТТ».

4.2. Цели и задачи, решаемые информационной системой

ИС «Бухгалтерский и кадровый учет», предназначена для автоматизации кадрового учета и расчета заработной платы в государственных учреждениях в соответствии с законодательством Российской Федерации.

ИС «Бухгалтерский и кадровый учет» решает следующие задачи:

- расчет заработной платы;
- исчисление регламентированных законодательством налогов и взносов с фонда оплаты труда;
- отражение начисленной зарплаты и налогов в затратах предприятия;
- управление денежными расчетами с персоналом;
- учет кадров и анализ кадрового состава;
- автоматизация кадрового делопроизводства;

ИС «Бухгалтерский и кадровый учет» включает в себя модуль «1С- Отчетность», который решает задачи по отправке реестров сведений:

- реестр сведений в ФСС о пособиях по нетрудоспособности;
- реестр сведений в ФСС о ежемесячных пособиях по уходу;
- реестр сведений в ФСС о пособиях при рождении ребенка.

4.3. Описание структурно-функциональных характеристик информационной системы

4.3.1. Структурная схема информационной системы

На рисунке 1 представлена структурная схема ИС «Бухгалтерский и кадровый учет».

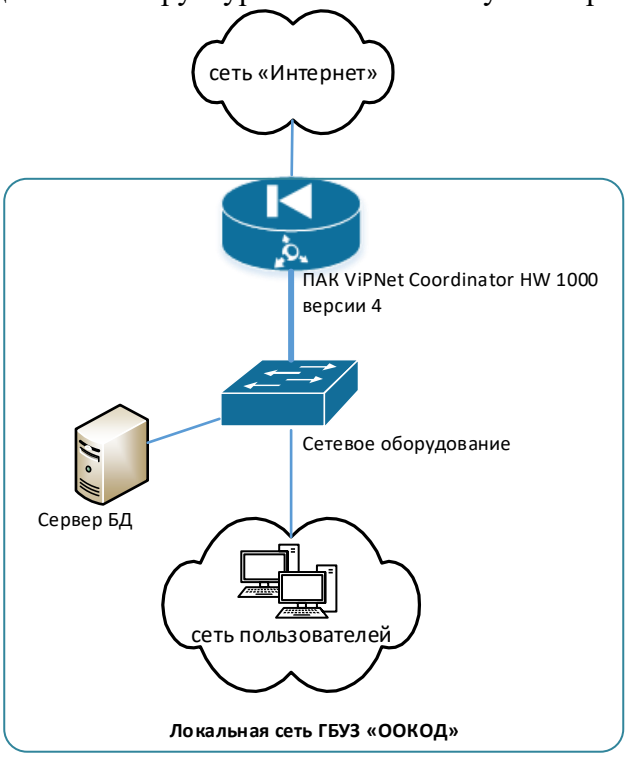

Рисунок 1 – Структурная схема ИС «Бухгалтерский и кадровый учет»

Программным обеспечением, реализующим технологические процессы обработки информации ИС «Бухгалтерский и кадровый учет» (далее – «ИС»), являются программы «1С: Бухгалтерия государственного учреждения» и «1С: Зарплата» фирмы «1С».

В ГАПОУ «С-ИИТТ» развернут сервер БД «ИС». Клиентская часть представляет собой автоматизированные рабочие места (далее - АРМ) работников ГАПОУ «С-ИИТТ» с установленным клиентским программным обеспечением «ИС».

БД «ИС» располагается в ГАПОУ «С-ИИТТ» на выделенном сервере.

ИС «Бухгалтерский и кадровый учет», реализовано на основе клиент-серверной архитектуры представляет собой локальную информационную систему, обеспечивающую автоматизацию кадровой службы и бухгалтерии в ГАПОУ «С-ИИТТ».

Данные, обрабатываемые в ИС «Бухгалтерский и кадровый учет», хранятся в ГАПОУ «С-ИИТТ» на сервере БД «ИС».

4.3.2. Состав информационной системы

ИС «Бухгалтерский и кадровый учет» представляет собой совокупность общесистемного, прикладного и специализированного программного обеспечения, средств вычислительной техники и сетевой инфраструктуры, функционирующих в целях автоматизации деятельности кадровой службы и бухгалтерии ГАПОУ «С-ИИТТ».

Основные структурные элементы ИС «Бухгалтерский и кадровый учет» приведены в Таблице 1.

Таблица 1 - Описание структурных элементов ИС «Бухгалтерский и кадровый учет»

Структурный элемент	Расположение
АРМ пользователя	ГАПОУ «С-ИИТТ»
Сервер БД	ГАПОУ «С-ИИТТ»,
Сетевое оборудование	ГАПОУ «С-ИИТТ»

4.3.3. Описание взаимодействия между сегментами информационной системы и взаимодействий с другими информационными и информационно-телекоммуникационными системами

Серверные компоненты ИС «Бухгалтерский и кадровый учет» и АРМ пользователей имеют подключение к сетям связи общего пользования, включая информационно телекоммуникационную сеть «Интернет».

Пользователи ИС «Бухгалтерский и кадровый учет» осуществляют доступ к БД «ИС» в рамках защищенной сети передачи данных министерства здравоохранения Оренбургской области.

ИС «Бухгалтерский и кадровый учет» так же взаимодействует с информационными системами Фонда социального страхования Российской Федерации, в рамках передачи реестров сведений о больничных листах посредством информационно телекоммуникационной сети «Интернет».

4.3.4. Объекты защиты информационной системы

Объектами воздействия являются объекты информационной системы, на которые может быть направлена угроза информационной безопасности. Состав объектов воздействия зависит от применяемых в информационной системе технологий обработки информации.

В Таблице 2 представлены разрешенные и запрещенные к применению технологии обработки информации и актуальные для ИС объекты воздействия, являющиеся объектами защиты, в соответствии с данными БДУ ФСТЭК России.

Таблица 2 – Перечень объектов воздействия ИС «Бухгалтерский и кадровый учет»

№ п/п	Объект воздействия	Примечание	Применимость технологии
1.	Аппаратное устройство (аппаратное средство, аппаратное обеспечение, техническое средство, средство вычислительной техники): Рабочая станция	Является объектом защиты	Технология разрешена к применению
2.	Аппаратное устройство (аппаратное средство, аппаратное обеспечение,	Является объектом защиты	Технология разрешена к применению

№ п/п	Объект воздействия	Примечание	Применимость технологии
	техническое средство, средство вычислительной техники): Сервер		
3.	Машинный носитель информации	Является объектом защиты	Технология разрешена к применению
4.	Носитель информации		
5.	Микропрограммное обеспечение	Является объектом защиты	Технология разрешена к применению
6.	Микропрограммное обеспечение BIOS/UEFI		
7.	Микропрограммное и аппаратное обеспечение BIOS/UEFI		
8.	Системное программное обеспечение	Является объектом защиты	Технология разрешена к применению
9.	Системное программное обеспечение, использующее реестр		
10.	Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)		
11.	Прикладное программное обеспечение	Является объектом защиты	Технология разрешена к применению
12.	Средства защиты информации	Является объектом защиты	Технология разрешена к применению
13.	Программно-аппаратные средства со встроенными функциями защиты		
14.	База данных	Является объектом защиты	Технология разрешена к применению
15.	Защищаемые данные	Является объектом защиты	Технология разрешена к применению
16.	Объекты файловой системы	Является объектом защиты	Технология разрешена к применению
17.	Файлы		
18.	Реестр	Является объектом защиты	Технология разрешена к применению
19.	Метаданные	Является объектом защиты	Технология разрешена к применению
20.	Аутентификационные данные пользователя	Является объектом защиты	Технология разрешена к применению
21.	Учётные данные пользователя		
22.	Сетевое оборудование	Является объектом защиты	Технология разрешена к применению
23.	Сетевой узел		
24.	Сетевое программное обеспечение		
25.	Сетевой трафик		
26.	Одноразовые пароли	Не является объектом воздействия	Технология использования одноразовых паролей запрещена к применению

№ п/п	Объект воздействия	Примечание	Применимость технологии
27.	Беспроводные технологии связи	Не является объектом воздействия	Беспроводные технологии связи запрещены к применению
28.	Каналы связи (передачи) данных	Является объектом защиты	Технология разрешена к применению
29.	Информационная система	Является объектом защиты	Технология разрешена к применению
30.	Инфраструктура информационных систем	Является объектом защиты	Технология разрешена к применению
31.	Технические средства воздушного кондиционирования серверного сегмента		
32.	Гипервизор	Не является объектом воздействия	Технологии гипервизора, ВМ и ВУ запрещены к применению
33.	Консоль управления гипервизором		
34.	Виртуальная машина		
35.	Образ виртуальной машины		
36.	Виртуальные устройства, виртуальные устройства хранения данных, виртуальные устройства хранения, обработки и передачи данных		
37.	Виртуальные диски		
38.	Вычислительные узлы суперкомпьютера	Не является объектом воздействия	Суперкомпьютерные технологии запрещены к применению
39.	Система хранения данных суперкомпьютера		
40.	Каналы передачи данных суперкомпьютера		
41.	Хранилище больших данных	Не является объектом воздействия	Технология больших данных запрещена к применению
42.	Узлы хранилища больших данных		
43.	Система разграничения доступа хранилища больших данных		
44.	Грид-система	Не является объектом воздействия	Грид-технология запрещена к применению
45.	Ресурсные центры грид-системы		
46.	Узлы грид-системы		
47.	Облачная система	Не является объектом воздействия	Облачные технологии запрещены к применению
48.	Облачная инфраструктура		
49.	Облачная инфраструктура, созданная с использованием технологий виртуализации		
50.	Консоль управления облачной инфраструктурой		
51.	Облачный сервер		
52.	Информационная система, иммигрированная в облако		
53.	Мобильное устройство (аппаратное устройство)	Не является объектом воздействия	Технологии использования мобильных устройств запрещены к применению
54.	Мобильные устройства (программное обеспечение)		
55.	Мобильное устройство и запущенные на нем приложения (программное обеспечение, аппаратное устройство)		
56.	Данные пользователя мобильного устройства (аппаратное устройство)		

№ п/п	Объект воздействия	Примечание	Применимость технологии
57.	Программное обеспечение автоматизированной системы управления технологическими процессами	Не является объектом воздействия	Технология автоматизированных систем управления производством запрещена к применению
58.	Программируемые логические контроллеры		
59.	Распределённые системы контроля		
60.	Управленческие системы и другие программные средства контроля		
61.	Ключевая система информационной инфраструктуры	Не является объектом воздействия	Технология управления критически важным объектом (процессом) запрещена к применению
62.	Модели машинного обучения	Не является объектом воздействия	Технологии машинного обучения и искусственного интеллекта запрещены к применению
63.	Обучающие данные машинного обучения		
64.	Программное обеспечение (программы), использующее машинное обучение		
65.	Программное обеспечение (программы), реализующие технологии искусственного интеллекта		

Исходя из применяемых технологий обработки информации и данных, приведённых в Таблице 2, можно сделать следующие выводы:

1) Применяемые объекты воздействия ИС «Бухгалтерский и кадровый учет» являются объектами защиты.

2) Объектами защиты ИС «Бухгалтерский и кадровый учет» являются:

– серверное оборудование;
– рабочие станции пользователей ИС «Бухгалтерский и кадровый учет»;
– сетевое оборудование для организации каналов связи между элементами ИС «Бухгалтерский и кадровый учет»;
– каналы связи между элементами ИС «Бухгалтерский и кадровый учет»;
– сетевые узлы ИС «Бухгалтерский и кадровый учет»;
– носители информации;
– системное программное обеспечение ИС «Бухгалтерский и кадровый учет»;
– прикладное программное обеспечение ИС «Бухгалтерский и кадровый учет»;
– сетевое программное обеспечение ИС «Бухгалтерский и кадровый учет»;
– аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI;
– средства защиты информации (в т.ч. программно-аппаратные средства со встроенными функциями защиты информации);
– инфраструктура ИС (в т.ч. технические средства воздушного кондиционирования серверного сегмента).

3) В ИС «Бухгалтерский и кадровый учет» подлежат защите следующие типы данных:

– метаданные;
– базы данных ИС «Бухгалтерский и кадровый учет»;
– защищаемые данные (в т.ч. обрабатываемые персональные данные, сведения о сетевых адресах, правилах маршрутизации и прочая информация, позволяющая раскрыть структуру ИС);
– реестр;
– объекты файловой системы;

– учетные и аутентификационные данные пользователей и администраторов;
– сетевой трафик.

4) В ИС «Бухгалтерский и кадровый учет» неприменимыми (запрещенными к применению) технологиями являются:

- гипервизор;
- консоль управления гипервизором;
- виртуальная машина;
- образ виртуальной машины;
- виртуальные устройства;
- виртуальные устройства хранения данных, виртуальные устройства хранения, обработки и передачи данных;
- виртуальные диски;
- беспроводные технологии связи;
- суперкомпьютерные технологии;
- технология больших данных;
- грид-технология;
- облачные технологии;
- технологии использования мобильных устройств;
- технология автоматизированных систем управления производством;
- технология управления критически важным объектом (процессом);
- технологии одноразовых паролей;
- технологии машинного обучения и искусственного интеллекта;
- технологии центров обработки данных.

4.3.5. Описание технологии обработки информации

Схема прохождения информации в ИС «Бухгалтерский и кадровый учет» представлена на рисунке 2.

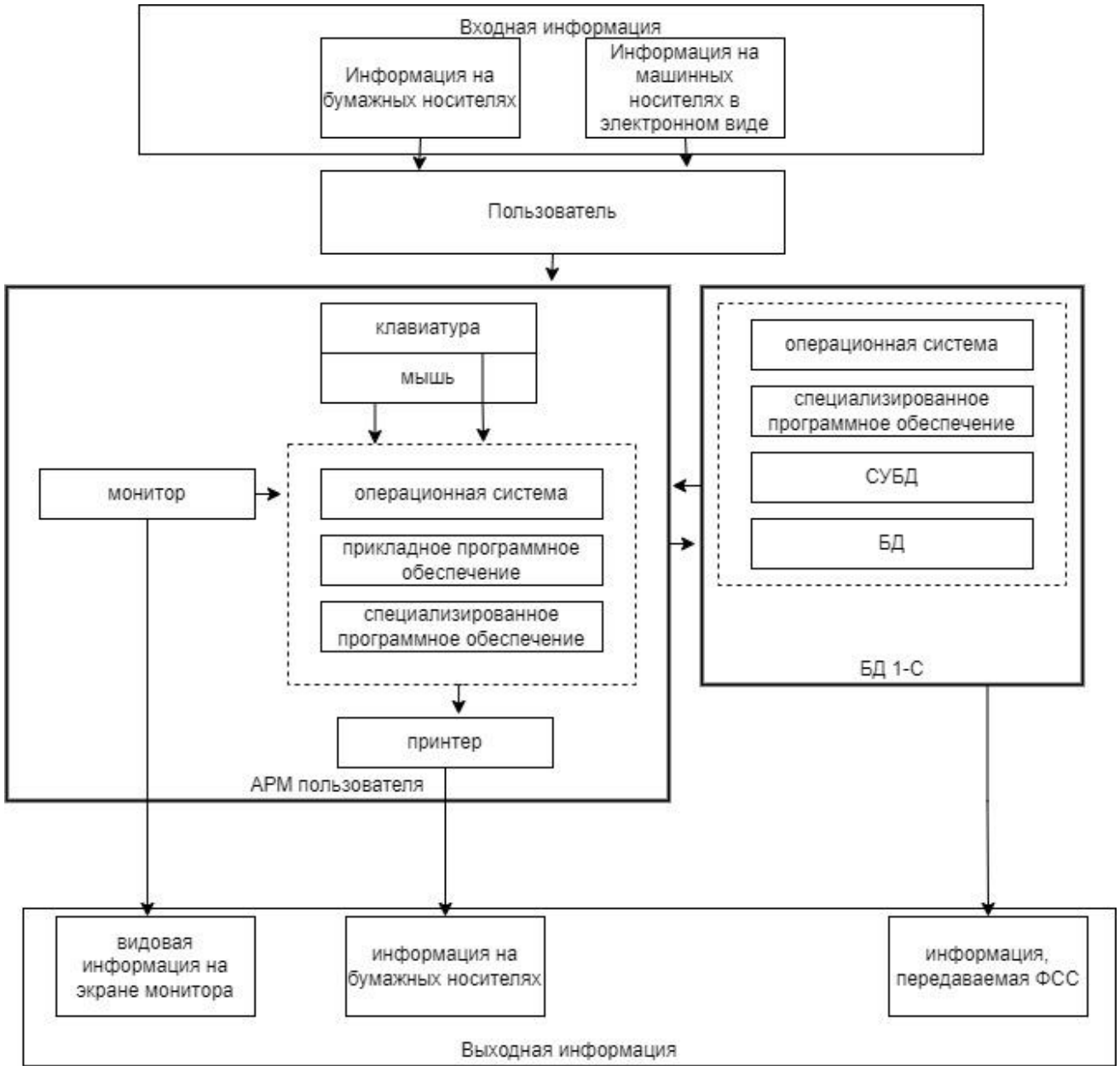

Рисунок 2 – Схема информационных потоков в ИС «Бухгалтерский и кадровый учет»

Входной информацией ИС, содержащей конфиденциальные сведения, может быть информация на бумажных носителях, а также информация, поступающая из информационных систем ФСС в формате электронного документа.

Ввод информации в ИС осуществляется пользователем вручную с использованием клавиатуры и манипулятора типа «мышь».

Хранение информации, обрабатываемой в образовательном учреждении в рамках ИС «Бухгалтерский и кадровый учет», осуществляется в БД на сервере образовательного учреждения.

Выходной информацией являются подготовленные в ИС и распечатанные документы на бумажном носителе, файлы в формате электронного документа на машинных носителях, видовая информация на экране монитора, а также информация, передаваемая в ФСС.

Выходная информация может содержаться на бумажных носителях, несъемных (внутренних) носителях информации.

4.4. Сведения о классификации информационной системы

В соответствии с Актом определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных, утвержденным директором ГАПОУ «С-ИИТТ» от 03.08.2023, ИС «Бухгалтерский и кадровый учет» имеет 4-й уровень защищенности ПДн:

- в ИСПДн обрабатываются ПДн, относящиеся к иным категориям ПДн;

– в ИСПДн одновременно обрабатываются ПДн в количестве менее 100 000 субъектов ПДн;

– для ИСПДн актуальны угрозы 3-го типа.

5. Источники угроз информационной безопасности

5.1. Определение источников угроз безопасности

Нарушение свойств безопасности информации, содержащейся в ИС «Бухгалтерский и кадровый учет», и возникновение неприемлемых негативных последствий может наступить в результате действий субъектов (физических лиц, организаций) или возникновения явлений (техногенные аварии, стихийные бедствия, иные природные явления).

Таким образом, можно выделить следующие типы источников угроз:

– техногенные источники;

– стихийные источники;

– антропогенные источники.

5.1.1. Угрозы техногенных источников

Техногенные источники угроз могут являться причиной отказов или сбоев в работе технических средств или программного обеспечения и напрямую зависят от таких свойств технических средств и программного обеспечения, как надежность и отказоустойчивость.

Техногенные угрозы могут быть обусловлены:

– низким качеством (надежностью) технических, программных или программно-технических средств;

– низким качеством (надежностью) сетей связи и (или) услуг связи;

– отсутствием или низкой эффективностью систем резервирования или дублирования программно-технических и технических средств;

– низким качеством (надежностью) инженерных систем (электроснабжения, охранных систем и т.д.);

– низким качеством обслуживания со стороны обслуживающих организаций и лиц;

– ошибками в программном обеспечении.

Для ИС «Бухгалтерский и кадровый учет» можно выделить следующие виды техногенных источников угроз безопасности информации:

1) Внешние техногенные источники:

– средства и линии связи;

– сети инженерных коммуникаций.

2) Внутренние техногенные источники:

– основные технические средства обработки информации (серверное оборудование, оборудование рабочих станций пользователей);

– вспомогательные технические средства обработки информации (сетевое оборудование, каналообразующее оборудование, инженерные системы (электроснабжения, охранных систем и т.д.), расположенные в помещениях, где находится оборудование ИС «Бухгалтерский и кадровый учет»;

– программное обеспечение.

Приведенные техногенные источники угроз безопасности информации могут привести к нарушению целостности и доступности обрабатываемой в ИС «Бухгалтерский и кадровый учет» информации.

5.1.2. Угрозы стихийных источников

Стихийные источники являются внешними по отношению к защищаемому объекту и под ними, прежде всего, понимаются природные катаклизмы: пожары, землетрясения, ураганы, наводнения, различные непредвиденные обстоятельства. Воздействие на информационную систему стихийных источников отличается непредсказуемостью, трудностью прогнозирования и противодействия им.

Для ИС «Бухгалтерский и кадровый учет» угрозы, связанные с действием стихийных источников, могут привести к нарушению целостности и доступности обрабатываемой в системе информации.

5.1.3. Антропогенные источники угроз

Антропогенные источники угроз связаны с преднамеренными или непреднамеренными действиями лиц, которые могут привести к нарушению безопасности информации, обрабатываемой в ИС «Бухгалтерский и кадровый учет».

Последствия в результате действия антропогенных источников угроз могут привести к нарушению конфиденциальности, целостности и доступности обрабатываемой в ИС «Бухгалтерский и кадровый учет» информации.

Угрозы, связанные с действиями антропогенных источников, являются наиболее актуальными для ИС «Бухгалтерский и кадровый учет». Типы и виды антропогенных источников (нарушителей), их возможности и потенциал рассмотрены в разделе 6 настоящей Модели угроз.

6. Модель нарушителя безопасности информации

6.1. Модель нарушителя в соответствии с методическими документами ФСТЭК России

6.1.1. Категории нарушителей

В зависимости от имеющихся прав и возможностей нарушители подразделяются на два типа, представленные в Таблице 3.

Таблица 3 – Типы нарушителей

№	Тип нарушителя	Описание
Ext	Внешние нарушители	Субъекты, не имеющие полномочий по доступу к информационным ресурсам и компонентам ИС
Int	Внутренние нарушители	Субъекты, имеющие полномочия по доступу к информационным ресурсам и компонентам ИС

Для ИС «Бухгалтерский и кадровый учет» актуальными являются как внутренние нарушители, так и внешние нарушители, поскольку ИС «Бухгалтерский и кадровый учет» имеет взаимодействие с сетью Интернет.

6.1.2. Виды нарушителей и возможные цели реализации угроз нарушителями

В Таблице 4 приведены виды внешних нарушителей и их возможные цели при реализации угроз безопасности информации в ИС «Бухгалтерский и кадровый учет».

Таблица 4 – Виды внешних нарушителей и их возможные цели реализации угроз

№	Вид нарушителя	Возможные цели внешнего нарушителя
Ext1	Специальные службы иностранных государств	– Нанесение ущерба государству, отдельным его сферам (областям) деятельности или секторам экономики – Нарушение или прекращение функционирования, дискредитация деятельности органов государственной власти, организаций – Нарушение работоспособности систем и сетей органов государственной власти – Внедрение скрытых функций в продукцию на этапе разработки, производства, поставки
Ext2	Террористические, экстремистские организации	– Нарушение или прекращение функционирования, дискредитация деятельности органов государственной власти, организаций – Нарушение работоспособности систем и сетей органов государственной власти
Ext3	Преступные группы	– Искажение информации для получения финансовой выгоды

№	Вид нарушителя	Возможные цели внешнего нарушителя
		– Рассылка информационных сообщений с использованием вычислительных мощностей оператора и(или) от его имени – Получение доступа к системам и сетям с целью незаконного использования вычислительных мощностей – Получение доступа к системам и сетям с целью дальнейшей продажи доступа – Кража конфиденциальной информации – Незаконное обогащение путем вымогательства денежных средств за восстановление доступа к заблокированным данным
Ext4	Физические лица	– Тестирование хакерских инструментов или апробация описанных способов осуществления атак – Нарушение работоспособности систем и сетей по причинам личной неприязни – Кража конфиденциальной информации

В Таблице 5 приведены виды внутренних нарушителей и их возможные цели при реализации угроз безопасности информации в ИС «Бухгалтерский и кадровый учет».

Таблица 5 – Виды внутренних нарушителей и их возможные цели реализации угроз

№	Вид нарушителя	Возможные цели внутреннего нарушителя
Int1	Разработчики, производители, поставщики программных, программно-аппаратных средств	– Внедрение скрытых функций в продукцию на этапе разработки, производства, поставки
Int2	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	– Внедрение скрытых функций в компоненты систем и сетей на этапе эксплуатации, ремонта – Кража конфиденциальной информации – Непреднамеренные, неосторожные или неквалифицированные действия
Int3	Лица, привлекаемые для администрирования (управления)	– Кража конфиденциальной информации – Непреднамеренные, неосторожные или неквалифицированные действия
Int4	Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	– Кража конфиденциальной информации – Непреднамеренные, неосторожные или неквалифицированные действия
Int5	Привилегированные пользователи	– Кража конфиденциальной информации – Непреднамеренные, неосторожные или неквалифицированные действия
Int6	Непривилегированные пользователи	– Кража конфиденциальной информации – Непреднамеренные, неосторожные или неквалифицированные действия

6.1.3. Возможности нарушителей

Возможности нарушителей (их потенциал) определяются компетентностью и оснащенностью, требуемыми им для реализации угроз безопасности информации. Уровни возможностей нарушителей приведены в Таблице 6.

Таблица 6 – Возможности (потенциал) нарушителей

№	Возможности (потенциал) нарушителя	Описание возможностей нарушителя по реализации угроз	Вид нарушителя		Предположение об актуальности нарушителя
1	Нарушитель, обладающий низким потенциалом	Наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей. Возможность реализовывать только известные угрозы и компьютерные атаки, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов. Базовые компьютерные знания и навыки на уровне пользователя	Ext4	Физические лица	актуален
			Int4	Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	актуален
			Int5	Привилегированные пользователи	актуален
			Int6	Непривилегированные пользователи	актуален
2	Нарушитель, обладающий средним потенциалом	Наличие возможностей уровня группы лиц/организации по разработке и использованию специальных средств эксплуатации уязвимостей. Возможность реализовывать сценарии угроз и компьютерные атаки, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети Интернет, или самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей. Практические знания о функционировании систем и сетей, операционных	Ext2	Террористические, экстремистские организации	не актуален
			Ext3	Преступные группы	актуален
			Int1	Разработчики, производители, поставщики программных, программно-аппаратных средств	не актуален
			Int2	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	актуален
			Int3	Лица, привлекаемые для администрирования (управления)	актуален

№	Возможности (потенциал) нарушителя	Описание возможностей нарушителя по реализации угроз	Вид нарушителя		Предположение об актуальности нарушителя
		систем, а также знания защитных механизмов.			
3	Нарушитель, обладающий высоким потенциалом	Наличие возможностей уровня предприятия/группы предприятий/государства по разработке и использованию специальных средств эксплуатации уязвимостей. Практически неограниченные возможности реализовывать сценарии угроз и компьютерные атаки, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей. Возможность получения доступа к исходному коду ПО для получения сведений об уязвимостях «нулевого дня». Возможность внедрения закладок. Возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций. Возможность создания и применения специальных технических средств для добывания информации, распространяющейся в виде физических полей или явлений. Возможность долговременно и незаметно для оператора системы реализовывать угрозы безопасности информации. Исключительные знания и практические навыки	Ext1	Специальные службы иностранных государств	не актуален

№	Возможности (потенциал) нарушителя	Описание возможностей нарушителя по реализации угроз	Вид нарушителя		Предположение об актуальности нарушителя
		о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также о конкретных защитных механизмах.			

Предполагается, что с целью повышения возможностей при реализации угроз отдельные виды актуальных нарушителей с низким потенциалом могут вступать в сговор с другими актуальными видами нарушителей, что приводит к появлению возможностей уровня группы лиц/организации и повышению потенциала нарушителя до среднего.

Предполагается, что нарушители при подготовке и создании методов и средств реализации угроз не будут привлекать и применять:

– специализированные научные;

– специально разработанные средства, в том числе обеспечивающие скрытное проникновение;

– специальные технические средства для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

Вышеизложенные предположения позволяют исключить из числа вероятных внешних и внутренних нарушителей с высоким потенциалом, к которым относятся специальные службы иностранных государств (Ext1), а также среди нарушителей со средним потенциалом террористические, экстремистские организации (Ext 2), имеющих возможность привлекать специалистов с опытом разработки и анализа средств защиты информации, а так же и разработчиков, производителей, поставщиков программных, программно-аппаратных средств (Int 1), ввиду отсутствия их заинтересованности.

6.1.4. Актуальные нарушители

Учитывая информацию, приведенную в разделах 6.1.1 – 6.1.3 настоящей Модели угроз, можно выделить следующие актуальные для ИС «Бухгалтерский и кадровый учет» виды нарушителей безопасности информации.

Таблица 7 – Актуальные нарушители

№	Вид нарушителя	Возможности (потенциал) нарушителя
Внешние нарушители		
Ext3	Преступные группы	Средний потенциал
Ext4	Физические лица	Низкий потенциал
Внутренние нарушители		
Int2	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	Средний потенциал
Int3	Лица, привлекаемые для администрирования (управления)	Средний потенциал
Int4	Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	Низкий потенциал
Int5	Привилегированные пользователи	Низкий потенциал
Int6	Непривилегированные пользователи	Низкий потенциал

Нарушитель с высоким потенциалом не является актуальным в виду недостаточной значимости информации, обрабатываемой в ИС «Бухгалтерский и кадровый учет» для данного вида нарушителя.

Таким образом, для ИС «Бухгалтерский и кадровый учет» актуальными будут являться:

- внешний нарушитель с низким потенциалом;
- внутренний нарушитель с низким потенциалом;
- внешний нарушитель со средним потенциалом;
- внутренний нарушитель со средним потенциалом.

6.2. Модель нарушителя в соответствии с методическими документами ФСБ России

6.2.1. Описание объектов защиты

К объектам защиты относятся:

- персональные данные, содержащиеся в ИС «Бухгалтерский и кадровый учет»;
- информация, содержащаяся в базе данных ИС «Бухгалтерский и кадровый учет» и электронных документах, создаваемых на АРМ из состава ИС «Бухгалтерский и кадровый учет», в отношении которой установлен режим конфиденциальности;
- СКЗИ;
- среда функционирования СКЗИ (далее - СФ);
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, журналы, издания, технические документы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

6.2.2. Определение возможностей нарушителя

В Таблице 8 приведены категории нарушителей и их возможности по реализации атак.

Таблица 8 – Категории нарушителей и их возможности по реализации атак

Категория нарушителя	Обобщенные возможности нарушителя	Да/нет
Н1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
Н2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
Н3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования	Да
Н4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения, и наводок СКЗИ)	Нет
Н5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области	Нет

Категория нарушителя	Обобщенные возможности нарушителя	Да/нет
	использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	
Н6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Нет

6.2.3. Уточнение возможностей нарушителя и направления атак

В Таблице 9 приведены уточненные возможности нарушителей и направления атак в соответствии с методическими рекомендациями ФСБ России, а также обоснования признания уточненных возможностей нарушителей и направлений атак неактуальными для ИС «Бухгалтерский и кадровый учет».

Таблица 9 – Актуальность использования возможностей нарушителей для реализации атак

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования	Обоснование отсутствия
1.1.	Проведение атаки при нахождении в пределах контролируемой зоны	актуально	
1.2.	Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, на которых реализованы СКЗИ и СФ.	актуально	
1.3.	Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	актуально	
1.4.	Использование штатных средств	актуально	

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования	Обоснование отсутствия
	ИС, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
2.1.	Физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	актуально	
2.2.	Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	актуально	
3.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности.
3.2.	Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности.
3.3.	Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности.

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования	Обоснование отсутствия
4.1.	Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; – высокая стоимость и сложность подготовки реализации возможности.
4.2.	Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3.	Возможность воздействовать на любые компоненты СКЗИ и СФ	не актуально	– не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

6.2.4. Классификация и характеристики нарушителей

Потенциальные нарушители (источники атак) могут быть поделены на следующие группы:

1. Внешние нарушители – физические лица, организации или группы лиц, осуществляющие атаки из-за пределов контролируемой зоны информационной системы (ими могут быть как лица, не имеющие право постоянного или разового доступа в КЗ, так и лица, имеющие такое право).

2. Внутренние нарушители – физические лица, осуществляющие атаки, находясь в пределах контролируемой зоны информационной системы (ими могут быть исключительно лица, имеющие право постоянного доступа в КЗ).

В Таблице 10 приведено описание категорий возможных нарушителей, их право доступа в контролируемую зону ИС «Бухгалтерский и кадровый учет», возможность или невозможность их доступа к объектам защиты и предположение о потенциальных источниках атак (актуальности нарушителя).

Таблица 10 – Категории нарушителей

Группа нарушителей	Категория нарушителя	Описание	Доступ в КЗ		Доступ к объектам защиты	Актуальность нарушителя
			постоянный	разовый		
Внешние	Н1	Внешние субъекты (физические лица)	нет	нет	нет	Является потенциальным источником атаки
Внутренние	Н2	Лица, обеспечивающие функционирование ИС и обслуживающие инфраструктуру ИС (охрана, работники	есть	есть	есть	Является потенциальным источником атаки

Группа наруш и телей	Катег ория нару шите ля	Описание	Доступ в КЗ		Доступ к объекта м защиты	Актуальность нарушителя
			постоянн ый	разовы й		
		инженерно-технических служб и т.д.)				
Внутре нние	Н3	Непривилегированны е пользователи ИС (работники ГАПОУ «С-ИИТТ», с полномочиями пользователя)	есть	есть	есть	Является потенциальным источником атаки
		Привилегированные пользователи ИС (работники ГАПОУ «С-ИИТТ» с полномочиями администратора)	есть	есть	есть	Является потенциальным источником атаки
Внешн ие	Н4	Разработчики, производители, поставщики программных, технических и программно-технических средств	нет	нет	нет	Не является потенциальным источником атаки. Данная категория лиц не заинтересована в проведении атак в связи с получением дохода от своей деятельности по поставке программных, технических и программно-технических средств для ИС и отнесена к доверенным лицам
		Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	нет	нет	нет	Не является потенциальным источником атаки. Данная категория лиц не заинтересована в проведении атак в связи с получением дохода от своей деятельности

Группа наруш и телей	Катег ория нару шите ля	Описание	Доступ в КЗ		Доступ к объекта м защиты	Актуальность нарушителя
			постоянн ый	разовы й		
						по ремонту, регламентному обслуживанию и иных работ в ИС и отнесена к доверенным лицам
Внешн ие	Н5	Террористические, экстремистские и преступные группировки	нет	нет	нет	Не является потенциальным источником атаки. Не осуществляется обработка сведений, составляющих государственну ю тайну, а также иных сведений, которые могут представлять интерес для реализации возможности
Внешн ие	Н6	Специальные службы иностранных государств	нет	нет	нет	Не является потенциальным источником атаки. Не осуществляется обработка сведений, составляющих государственну ю тайну, а также иных сведений, которые могут представлять интерес для реализации возможности

6.2.5. Актуальность применения средств криптографической защиты информации

Применение СКЗИ для защиты информации в ИС «Бухгалтерский и кадровый учет» необходимо в следующих случаях:

– если данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

– если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

ИС «Бухгалтерский и кадровый учет» является распределенной системой, узлы которой объединены каналами связи. Каналы связи, объединяющие узлы ИС «Бухгалтерский и кадровый учет» в единое информационное пространство, находятся за пределами контролируемых зон участников информационного обмена

Для защиты информации, передаваемой по каналам связи, от перехвата или несанкционированного доступа к ней целесообразно применять СКЗИ.

В соответствии с разделом 4.5 для ИС «Бухгалтерский и кадровый учет» определена необходимость обеспечения 3-го уровня защищенности ПДн. Согласно требованиям приказа ФСБ от 10.07.2014 № 378 в случае принятия решения о необходимости защиты ПДн с помощью СКЗИ для обеспечения требуемого уровня защищенности ПДн при их обработке в информационной системе необходимо использовать СКЗИ класса КС1 и выше.

В соответствии с изложенными выше предположениями о наличии возможностей у нарушителей на проведение атак и в соответствии с п.10 приказа ФСБ России от 10.07.2014 № 378 в ИС «Бухгалтерский и кадровый учет» целесообразно применение СКЗИ класса КС1.

7. Способы реализации угроз

В общем случае угрозы безопасности информации, обрабатываемой в информационной системе, могут быть реализованы за счет:

– несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

– несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

– несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

– несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

– несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

– воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

7.1. Угрозы, связанные с НСД к информации

Предполагается, что актуальным нарушителем могут быть реализованы угрозы, связанные с НСД к информации, обрабатываемой в ИС «Бухгалтерский и кадровый учет». При этом:

– несанкционированный доступ (далее - НСД) может быть следствием как случайных, так и преднамеренных действий нарушителя;

– нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от лиц, контролирующих соблюдение мер безопасности.

Внешние нарушители имеют возможность съема и перехвата информации с каналов связи ИС «Бухгалтерский и кадровый учет», по которым передаются данные и которые выходят за пределы КЗ.

Внешние нарушители могут реализовать угрозы безопасности за счет:

– НСД через АРМ, подключенные к сетям общего пользования (Интернет);

– НСД к информации с использованием вредоносных программ, программных закладок;

– НСД через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла оказываются за пределами КЗ (модернизация, сопровождение, ремонт, утилизация).

Внутренние нарушители могут реализовать угрозы безопасности за счет:

– легального доступа через АРМ и иные элементы инфраструктуры, входящие в состав ИС «Бухгалтерский и кадровый учет».

7.2. Угрозы утечки по техническим каналам

За счет реализации технических каналов утечки информации возможно возникновение следующих угроз:

– угроз утечки акустической (речевой) информации;

– угроз утечки видовой информации;

– угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Возникновение угроз утечки акустической (речевой) информации связано с голосовым воспроизведением информации, обрабатываемой в ИС «Бухгалтерский и кадровый учет», пользователями и обслуживающим персоналом.

Перехват акустической (речевой) информации возможен путем подслушивания переговоров нарушителем, находящимся в непосредственной близости с помещением, в

котором ведутся переговоры, а также с помощью специальной аппаратуры и устройств съема речевой информации.

Предполагается, что актуальный нарушитель не обладает специальной аппаратурой для съема речевой информации, а защита от непосредственного подслушивания переговоров нарушителем достигается организационными мерами. Также в ИС «Бухгалтерский и кадровый учет» не предусмотрены средства акустического ввода конфиденциальной информации.

Таким образом, угрозы утечки акустической (речевой) информации для ИС «Бухгалтерский и кадровый учет» возможны при непреднамеренном прослушивании, но при использовании специальных технических средств угрозы являются неактуальными.

Угрозы утечки видовой информации реализуются за счет просмотра обрабатываемой информации с экранов дисплеев и других устройств отображения средств вычислительной техники, входящих в состав информационной системы.

Предполагается, что актуальный нарушитель не обладает специальными электронными средствами съема видовой информации, а наиболее вероятной угрозой является несанкционированный просмотр информации путем непосредственного наблюдения в служебных помещениях либо вне помещения с расстояния прямой видимости с использованием оптических средств. Предотвращение несанкционированного просмотра информации с экранов дисплеев и других устройств отображения средств вычислительной техники ИС «Бухгалтерский и кадровый учет» достигается применением таких организационных мер, как расположение мониторов, исключающее просмотр экранов со стороны окон и входной двери, использование жалюзи (штор) на окнах.

Таким образом, угрозы утечки видовой информации для ИС «Бухгалтерский и кадровый учет» возможны при непреднамеренном просмотре, но с использованием специальных технических средств угрозы являются неактуальными.

Предполагается, что актуальный нарушитель не обладает специальными средствами регистрации, перехвата и съема побочных информативных электромагнитных полей, и электрических сигналов, возникающих при обработке информации техническими средствами, входящими в состав ИС «Бухгалтерский и кадровый учет», поэтому угрозы утечки информации по каналам ПЭМИН для ИС «Бухгалтерский и кадровый учет» являются неактуальными.

7.3. Угрозы специальных воздействий

Предполагается, что угрозы специальных воздействий на информационную систему путем химического, биологического, радиационного, термического, электромагнитного, акустического, механического воздействия не являются актуальными для ИС «Бухгалтерский и кадровый учет», поскольку актуальный нарушитель не обладает средствами и устройствами, позволяющими реализовать данный вид угроз, в системе не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации угроз специальных воздействий. Ещё одним фактором, подтверждающим неактуальность данного класса угроз, является высокая стоимость и сложность подготовки реализации угрозы. Реализация данной угрозы неактуальна, так как ее реализация может быть выполнена нарушителем с высоким потенциалом, который для ИС «Бухгалтерский и кадровый учет» не актуален.

8. Анализ последствий от нарушения свойств безопасности информации

В соответствии с решаемыми ИС «Бухгалтерский и кадровый учет» задачами, условиями эксплуатации ИС «Бухгалтерский и кадровый учет», значимостью обрабатываемой информации и значимостью самой системы нарушение свойств безопасности информации (конфиденциальности, целостности, доступности) может привести к различного рода негативным последствиям:

– незначительным негативным последствиям (последствия, не требующие финансовых затрат, не приводящие к угрозе жизни и здоровью человека, не приносящие ущерб в области обороны, безопасности и правопорядка, не приводящие к политическому ущербу);

– умеренным негативным последствиям (последствия, требующие незначительных финансовых затрат, не приводящие к угрозе жизни и здоровью человека, не приносящие ущерб в области обороны, безопасности и правопорядка, не приводящие к политическому ущербу);

– существенным негативным последствиям (последствия, требующие значительных финансовых затрат, приводящие к угрозе жизни и здоровью человека, приносящие ущерб в области обороны, безопасности и правопорядка, приводящие к политическому ущербу).

При обработке в информационной системе двух и более видов информации негативные последствия целесообразно определять отдельно для каждого вида защищаемой информации, применительно к каждому виду ущерба.

В ИС «Бухгалтерский и кадровый учет» можно выделить следующие категории защищаемой информации:

– персональные данные в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– технологическая информация, включая информацию о системе защиты информации в ИС «Бухгалтерский и кадровый учет».

При этом для разных обладателей информации (обладателя информации или оператора ИС и субъектов ПДн, данные которых обрабатываются в системе) могут быть выделены различные виды ущерба и последствия от нарушения свойств безопасности информации (конфиденциальности, целостности и доступности).

Сводная информация по определению степени негативных последствий от нарушения свойств безопасности информации (конфиденциальности, целостности и доступности) для разных категорий защищаемой информации, разных обладателей информации и различных видов ущерба приведена в Таблице 11.

Таблица 11 – Определение степени негативных последствий от нарушения свойств безопасности информации

Категория защищаемой информации	Обладатель информации	Вид ущерба	Свойство информации	Негативные последствия	Степень негативных последствий
Персональные данные	Оператор	Социальный	Конфиденциальность	–Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. –Появление негативных публикаций в общедоступных источниках.	Незначительные негативные последствия
			Целостность	– Нарушение целостности не приводит к нанесению ущерба	-
			Доступность	– Нарушение доступности не приводит к нанесению ущерба	-
		Репутационный	Конфиденциальность	– Нарушение законодательных и подзаконных актов. – Нарушение деловой репутации.	Незначительные негативные последствия

Категория защищаемой информации	Обладатель информации	Вид ущерба	Свойство информации	Негативные последствия	Степень негативных последствий
				– Дискредитация работников. – Утрата доверия.	
			Целостность	– Нарушение целостности не приводит к нанесению ущерба	-
			Доступность	– Нарушение доступности не приводит к нанесению ущерба	-
		Технологический	Конфиденциальность	– Нарушение конфиденциальности не приводит к нанесению ущерба	-
			Целостность	– Нарушение целостности не приводит к нанесению ущерба	-
			Доступность	– Снижение эффективности решения задач (реализации функций) – Необходимость изменения (перестроения) внутренних процедур	Незначительные негативные последствия
	Субъект ПДн	Ущерб субъекту ПДн	Конфиденциальность	– Создание угрозы личной безопасности – Вторжение в частную жизнь – Моральный вред	Незначительные негативные последствия
			Целостность	– Создание угрозы здоровью	-
			Доступность	– Нарушение доступности не приводит к нанесению ущерба	-
Технологическая информация о системе защиты информации	Оператор	Экономический	Конфиденциальность	– Нарушение конфиденциальности не приводит к нанесению ущерба	-
			Целостность	– Нарушение целостности не приводит к нанесению ущерба	-

Категория защищаемой информации	Обладатель информации	Вид ущерба	Свойство информации	Негативные последствия	Степень негативных последствий
			Доступность	– Нарушение доступности не приводит к нанесению ущерба	-
		Технологический	Конфиденциальность	– Нарушение конфиденциальности и не приводит к нанесению ущерба	-
			Целостность	– Нарушение целостности не приводит к нанесению ущерба	-
			Доступность	– Нарушение доступности не приводит к нанесению ущерба	-

Анализ возможных последствий от нарушения свойств безопасности информации показал, что для ИС «Бухгалтерский и кадровый учет» критичными являются нарушения всех трех свойств безопасности информации (конфиденциальности, целостности и доступности), поскольку их нарушение в результате реализации угроз может привести к негативным последствиям для обладателя информации. Следовательно, в ИС «Бухгалтерский и кадровый учет» необходимо обеспечить защиту от угроз, направленных на нарушение конфиденциальности, целостности и доступности информации.

9. Определение актуальных угроз безопасности информации

Угрозы безопасности информации определяются по результатам оценки:

- возможностей (потенциала) внешних и внутренних нарушителей;
- анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации;
- последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Результаты оценки возможностей (потенциала) нарушителей, включающие описание возможностей нарушителей и выводы об актуальных нарушителях для ИС «Бухгалтерский и кадровый учет», приведены в разделе 6.1. настоящей Модели угроз.

Анализ последствий от нарушения свойств безопасности информации в случае реализации угроз безопасности информации для ИС «Бухгалтерский и кадровый учет» приведен в разделе 8 настоящей Модели угроз.

Сводные данные по определению актуальных угроз безопасности информации ИС «Бухгалтерский и кадровый учет» приведены в Приложении к настоящей Модели угроз.

Перечень угроз сформирован с использованием Банка данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

Приложение. Угрозы безопасности информации

Для ИС «Бухгалтерский и кадровый учет» необходимо обеспечить защиту от угроз, направленных на нарушение конфиденциальности, целостности и доступности информации.

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)[1]	Объект воздействия	Актуальность УБИ	Примечание
001	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 администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы	ВнеС, ВнуС	Ресурсные центры грид-системы	неактуальная	Грид-технология не применима для ИС
002	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.	ВнеС	Сетевой трафик	неактуальная	Грид-технология не применима для ИС

[1] – ВнеН – внешний нарушитель с низким потенциалом;
ВнуН – внутренний нарушитель с низким потенциалом;
ВнеС – внешний нарушитель со средним потенциалом;
ВнуС – внутренний нарушитель со средним потенциалом;
ВнеВ – внешний нарушитель с высоким потенциалом;
ВнуВ – внутренний нарушитель с высоким потенциалом.

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)[1]	Объект воздействия	Актуальность УБИ	Примечание
		Реализация данной угрозы возможна при условии наличия у нарушителя: сил и средств, достаточных для компенсации чрезвычайной распределённости грид-заданий между узлами грид-системы; привилегий, достаточных для перехвата трафика сети передачи данных между элементами (узлами) грид-системы				
003	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. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки	ВнеС	Метаданные, системное программное обеспечение	актуальная	-
004	Угроза аппаратного сброса пароля BIOS	Угроза заключается в возможности сброса паролей, установленных в BIOS/UEFI без прохождения процедуры авторизации в системе	ВнуН	Микропрограммное и аппаратное	актуальная	-

[1] – ВнеН – внешний нарушитель с низким потенциалом;
ВнуН – внутренний нарушитель с низким потенциалом;
ВнеС – внешний нарушитель со средним потенциалом;
ВнуС – внутренний нарушитель со средним потенциалом;
ВнеВ – внешний нарушитель с высоким потенциалом;
ВнуВ – внутренний нарушитель с высоким потенциалом.

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)[1]	Объект воздействия	Актуальность УБИ	Примечание
		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		обеспечение BIOS/UEFI		
005	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	ВнуВ	Микропрограммное и аппаратное обеспечение BIOS/UEFI	неактуальная	Внутренний нарушитель с высоким потенциалом не актуален для ИС

[1] – ВнеН – внешний нарушитель с низким потенциалом;
ВнуН – внутренний нарушитель с низким потенциалом;
ВнеС – внешний нарушитель со средним потенциалом;
ВнуС – внутренний нарушитель со средним потенциалом;
ВнеВ – внешний нарушитель с высоким потенциалом;
ВнуВ – внутренний нарушитель с высоким потенциалом.

[1] – ВнеН – внешний нарушитель с низким потенциалом;
ВнуН – внутренний нарушитель с низким потенциалом;
ВнеС – внешний нарушитель со средним потенциалом;
ВнуС – внутренний нарушитель со средним потенциалом;
ВнеВ – внешний нарушитель с высоким потенциалом;
ВнуВ – внутренний нарушитель с высоким потенциалом.

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
006	Угроза внедрения кода или данных	Угроза заключается в возможности внедрения нарушителем в дискредитируемую информационную систему или IoT-устройство вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также в возможности несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую информационную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов, и блокирования работы устройства при выполнении определенных команд. Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа; наличием открытого Telnet-порта на IoT-устройстве (только для IoT-устройств). Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников;	ВнеН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		при наличии у него привилегий установки программного обеспечения; в случае неизмененных владельцем учетных данных IoT-устройства (заводских пароля и логина)				
007	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	ВнеС, ВнуС	Информационная система, виртуальная машина, сетевое программное обеспечение, сетевой трафик	актуальная	-
008	Угроза восстановления аутентификационной информации	Угроза заключается в возможности доступа к данным пользователя в результате подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе, а также путём перехвата	ВнеН, ВнуН	Системное программное обеспечение, микропрограммное обеспечение,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		и повторного использования хэша пароля, для восстановления сеанса. Данная угроза обусловлена следующими недостатками: значительно меньшим объёмом данных хеш-кода аутентификационной информации по сравнению с ней самой (время подбора хеш-кодов меньше времени полного перебора аутентификационной информации); слабостями алгоритма расчёта хеш-кода, допускающими его повторное использование для выполнения успешной аутентификации. Реализация данной угрозы возможна с помощью специальных программных средств, а также в некоторых случаях – «вручную»		учётные данные пользователя		
009	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;	ВнуН	Микропрограммное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
010	Угроза выхода процесса за пределы виртуальной машины	Угроза заключается в возможности запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора. Данная угроза обусловлена уязвимостями программного обеспечения гипервизора, 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	ВнеС, ВнуС	Информационная система, сетевой узел, носитель информации, объекты файловой системы, учётные данные пользователя, образ виртуальной машины	неактуальная	Технология виртуализации не применима к ИС -

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		выполнять функции безопасности в отношении вредоносных программ, функционирующих под управлением собственного гипервизора				
011	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	ВнеН, ВнуН	Сетевой узел	неактуальная	Технология беспроводной связи не применима для ИС
012	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.	ВнуН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограм	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		мное обеспечение, метаданные, объекты файловой системы, реестр		
013	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	ВнуН	Микропрограммное обеспечение BIOS/UEFI	актуальная	-
014	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	ВнеН, ВнуН	Информационная система, сетевой узел, носитель информации, системное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		программное обеспечение, сетевое программное обеспечение, сетевой трафик		
015	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. 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,	ВнеН, ВнуН	Объекты файловой системы	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		обработка которых не предполагается с её помощью				
016	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	ВнеС	Сетевое программное обеспечение	актуальная	-
017	Угроза доступа/перехвата/изменения HTTP cookies	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации (учётным записям пользователей, сертификатам и т.п.), содержащейся в cookies-файлах, во время их хранения или передачи, в режиме чтения (раскрытие конфиденциальности) или записи (внесение изменений для реализации угрозы подмены доверенного пользователя).	ВнеН	Прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
018	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	ВнуН	Микропрограммное обеспечение BIOS/UEFI	актуальная	-
019	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	ВнеН	Сетевой узел, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
020	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	ВнуН	Облачная система, виртуальная машина	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		оказывает негативное влияние на репутацию поставщика облачных услуг				
021	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)	ВнеН	Облачная система	неактуальная	Облачная технология не применима для ИС
022	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.	ВнеН, ВнуН	Аппаратное обеспечение, системное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
023	Угроза изменения компонентов системы	Угроза заключается в возможности получения нарушителем доступа к сети, файлам, 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 и возможности подключения дополнительного периферийного оборудования	ВнуН	Информационная система, сервер, рабочая станция, виртуальная машина, системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	актуальная	-
024	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:	ВнуВ	Микропрограммное и аппаратное обеспечение BIOS/UEFI	неактуальная	Внутренний нарушитель с высоким потенциалом

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				не актуален для ИС
025	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	ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
026	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 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	ВнеС, ВнуС	Сетевой узел, сетевое программное обеспечение, сетевой трафик	актуальная	-
027	Угроза искажения вводимой и выводимой	Угроза заключается в возможности дезинформирования пользователей или автоматических систем управления путём	ВнеВ, ВнуН	Системное программное обеспечение,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	на периферийные устройства информации	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		прикладное программное обеспечение, сетевое программное обеспечение, аппаратное обеспечение		
028	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	ВнеН, ВнуН	Сетевой узел, объекты файловой системы, прикладное программное обеспечение, системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		условии наличия у нарушителя: возможности ввода произвольных данных в адресную строку; сведений о пути к защищаемому ресурсу; возможности изменения интерфейса ввода входных данных				
029	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	ВнеН, ВнуН	Вычислительные узлы суперкомпьютера	неактуальная	Суперкомпьютерная технология не применима для ИС
030	Угроза использования информации идентификации/аутенти	Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников или от информационного сервиса	ВнеС, ВнуН	Средства защиты информации, системное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	фикации, заданной по умолчанию	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 или тем, что при прохождении на информационном сервисе процедуры регистрации механизм автоматической генерации паролей выдает одинаковые или сходные пароли пользователям с похожими логинами. 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		программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, программно-аппаратные средства со встроенными функциями защиты		

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		защиты наличие у нарушителя сведений о логине используемом при регистрации атакуемым пользователем				
031	Угроза использования механизмов авторизации для повышения привилегий	Угроза заключается в возможности получения нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки. Данная угроза обусловлена слабостями мер разграничения доступа к программам и файлам. Реализация данной угрозы возможна в случае наличия у нарушителя каких-либо привилегий в системе	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-
032	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	ВнеС	Микропрограммное и аппаратное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений				
033	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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	актуальная	-
034	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	ВнеН, ВнуН	Системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		протоколов (заложенных в них алгоритмов), ошибками, допущенными в ходе реализации протоколов, или уязвимостями, внедряемыми автоматизированными средствами проектирования/разработки. Реализация данной угрозы возможна в случае наличия слабостей в протоколах сетевого/локального обмена данными				
035	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	ВнеВ	Микропрограммное обеспечение BIOS/UEFI	неактуальная	Внешний нарушитель с высоким потенциалом не актуален для ИС
036	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.	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		микропрограммное обеспечение		
037	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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	актуальная	-
038	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	ВнуН	Информационная система	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
039	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	ВнеС	Микропрограммное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
040	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. 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	ВнеН	Облачная система	неактуальная	Облачная технология не применима для ИС. Трансграничная передача защищаемой информации не осуществляется.
041	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	ВнеН	Сетевой узел, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		нарушитель имеет возможность отправки запросов и данных в дискредитируемую систему				
042	Угроза межсайтовой подделки запроса	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя. Данная угроза обусловлена уязвимостями браузеров, которые позволяют выполнять действия без подтверждения или аутентификации со стороны дискредитируемого пользователя. Реализация угрозы возможна в случае, если дискредитируемый пользователь сохраняет аутентификационную информацию с помощью браузера	ВнеС	Сетевой узел, сетевое программное обеспечение	актуальная	-
043	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	ВнеН, ВнуН	Облачная система, облачный сервер	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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 успешно реализованная угроза в отношении всего лишь одного облачного сервиса позволит нарушить доступность всей облачной системы				
044	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	ВнеС, ВнуС	Виртуальная машина, гипервизор	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		низких (по отношению к гипервизору) уровней функционирования системы				
045	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	ВнуН	Микропрограммное и аппаратное обеспечение BIOS/UEFI	актуальная	-
046	Угроза нарушения процедуры аутентификации субъектов виртуального	Угроза заключается в возможности подмены субъекта виртуального информационного взаимодействия, а также в возможности возникновения состояния неспособности осуществления такого взаимодействия.	ВнеН, ВнуН	Сетевой узел, сетевое программное обеспечение, метаданные,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	информационного 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		учётные данные пользователя		
047	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	ВнеС, ВнуС	Грид-система, сетевой трафик	неактуальная	Грид-технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		отдельных узлов грид-системы со стороны диспетчера задач грид-системы				
048	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; 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)	ВнеС, ВнуС	Образ виртуальной машины, сетевой узел, сетевое программное обеспечение, виртуальная машина	актуальная	-
049	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	ВнеН, ВнуН	Сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
050	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	ВнуН	Хранилище больших данных, метаданные	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
051	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.)	ВнуН	Рабочая станция, носитель информации, системное программное обеспечение, метаданные, объекты файловой системы, реестр	актуальная	-
052	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.	ВнеН	Облачная инфраструктура, виртуальная машина, аппаратное обеспечение, системное программное обеспечение	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
053	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	ВнуН	Микропрограммное обеспечение BIOS/UEFI	актуальная	-
054	Угроза недобросовестного исполнения обязательств	Угроза заключается в возможности раскрытия или повреждения целостности поставщиком облачных услуг защищаемой информации потребителей облачных услуг, невыполнения	ВнеН	Информационная система, сервер, носитель	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	поставщиками облачных услуг	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.		информации, метаданные, объекты файловой системы		
055	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	ВнеН, ВнуН	Облачная система, рабочая станция, сетевое программное обеспечение	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		получения нарушителем аутентификационной информации (при их вводе в общественных местах) легальных пользователей, или эксплуатации уязвимостей в средствах удалённого администрирования				
056	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 осуществлении переноса информационной системы в облако	ВнеН	Информационная система, иммигрированная в облако, облачная система	неактуальная	Облачная технология не применима для ИС
057	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	ВнуН	Хранилище больших данных, метаданные, защищаемые данные	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
058	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	ВнеН, ВнуН	Облачная система, консоль управления облачной инфраструктурой, облачная инфраструктура	неактуальная	Облачная технология не применима для ИС
059	Угроза неконтролируемого роста числа	Угроза заключается в возможности отказа легальным пользователям в выделении компьютерных ресурсов после осуществления	ВнеН, ВнуН	Информационная система, сервер	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	зарезервированных вычислительных ресурсов	нарушителем неправомерного резервирования всех свободных компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). 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				
060	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	ВнуН	Хранилище больших данных, метаданные, защищаемые данные	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
061	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	ВнуС	Сетевой трафик, база данных, сетевое программное обеспечение	актуальная	-
062	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 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	ВнеН	Сетевое программное обеспечение	актуальная	-
063	Угроза некорректного использования	Угроза заключается в возможности использования декларированных возможностей	ВнеС, ВнуС	Системное программное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	функционала программного и аппаратного обеспечения	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		обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, аппаратное обеспечение		
064	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	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		лицензируемым программным обеспечением использованы много раз				
065	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. 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)	ВнеН, ВнуН	Системное программное обеспечение	неактуальная	Облачная технология не применима для ИС
066	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	ВнеН	Облачная система	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		сторонами участвующими в оказании облачных услуг, а также отсутствия документального определения ответственности за несоблюдение требований безопасности				
067	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.	ВнуН	Аппаратное обеспечение, носители информации, объекты файловой системы	актуальная	-
068	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).	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		программное обеспечение, микропрограммное обеспечение, реестр		
069	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путём добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи. Данная угроза обусловлена слабостями сетевых протоколов, заключающимися в отсутствии проверки целостности и подлинности получаемых данных. Реализация данной угрозы возможна при условии осуществления нарушителем несанкционированного доступа к сетевому трафику	ВнеН	Сетевой трафик	актуальная	-
070	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	ВнуС	Облачная инфраструктура	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
071	Угроза несанкционированного восстановления удалённой защищаемой информации	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	ВнеН, ВнуН	Машинный носитель информации	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
072	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	ВнуН	Микропрограммное и аппаратное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера				
073	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. Реализация данной угрозы возможна при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования	ВнеС, ВнуС	Сетевое оборудование, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства	актуальная	-
074	Угроза несанкционированного доступа к аутентификационной информации	Угроза заключается в возможности извлечения паролей, имён пользователей или других учётных данных из оперативной памяти компьютера или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с машинных носителей информации	ВнеН, ВнуН	Системное программное обеспечение, объекты файловой системы, учётные данные	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
				пользователя, реестр, машинные носители информации		
075	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	ВнеН, ВнуН	Сетевое программное обеспечение, сетевой трафик, виртуальные устройства	актуальная	-
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им	ВнеС, ВнуС	Гипервизор	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети. Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данной угрозы возможна в одном из следующих случаев: наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин; наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью				
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том	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.	ВнеС, ВнуС	Сервер, рабочая станция, виртуальная машина, гипервизор, машинный	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	числе выделенного под виртуальное аппаратное обеспечение	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		носитель информации, метаданные		
078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации. Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых	ВнеН, ВнуН	Виртуальная машина	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами. Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия				
079	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 использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе	ВнеН, ВнуН	Виртуальная машина	неактуальная	Технология виртуализации не применима к ИС
080	Угроза несанкционированного доступа к защищаемым виртуальным	Угроза заключается в возможности удалённого осуществления нарушителем несанкционированного доступа к виртуальным устройствам из виртуальной и (или) физической	ВнеС, ВнуС	Виртуальные устройства хранения, обработки и	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	устройствам из виртуальной и (или) физической сети	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		передачи данных		
081	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 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	ВнеС	Узлы грид-системы	неактуальная	Грид-технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
082	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	ВнуС	Вычислительный узел суперкомпьютера	неактуальная	Суперкомпьютерная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
083	Угроза несанкционированного доступа к системе по беспроводным каналам	Угроза заключается в возможности получения нарушителем доступа к ресурсам всей дискредитируемой информационной системы через используемые в ее составе беспроводные каналы передачи данных. Данная угроза обусловлена слабостями протоколов идентификации/аутентификации (таких как WEP, WPA и WPA2, AES), используемых для доступа к беспроводному оборудованию. Реализация данной угрозы возможна при условии наличия у нарушителя специализированного программного обеспечения, реализующего функции эксплуатации уязвимостей протоколов идентификации/аутентификации беспроводных сетей, а также нахождения в точке приема сигналов дискредитируемой беспроводной сети	ВнеН	Сетевой узел, учётные данные пользователя, сетевой трафик, аппаратное обеспечение	неактуальная	Технологии беспроводной связи не применима для ИС
084	Угроза несанкционированного	Угроза заключается в возможности осуществления деструктивного программного	ВнеН, ВнуН	Виртуальные устройства	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	доступа к системе хранения данных из виртуальной и (или) физической сети	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 слабости технологий, использованных при построении системы хранения данных (сетевых технологий, технологий распределения информации и др.)		хранения данных, виртуальные диски		

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
085	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	ВнеС, ВнуС	Носитель информации, объекты файловой системы	актуальная	-
086	Угроза несанкционированного изменения аутентификационной информации	Угроза заключается в возможности осуществления неправомерного доступа нарушителем к аутентификационной информации других пользователей с помощью штатных средств операционной системы или	ВнеН, ВнуН	Системное программное обеспечение, объекты файловой	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		системы, учётные данные пользователя, реестр		
087	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	ВнеВ, ВнуН	Аппаратное обеспечение, микропрограммное обеспечение BIOS/UEFI	актуальная	-
088	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	ВнеН, ВнуН	Объекты файловой системы, машинный носитель информации	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		снятия копии в момент обработки защищаемой информации в нешифрованном виде				
089	Угроза несанкционированного редактирования реестра	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 Microsoft Windows, 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	ВнеН, ВнуН	Системное программное обеспечение, использующее реестр, реестр	актуальная	-
090	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	ВнеН, ВнуН	Системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
091	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	ВнеН, ВнуН	Метаданные, объекты файловой системы, реестр	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		расстояние, достаточное для оказания эффективного деструктивного воздействия				
092	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)	ВнеВ	Информационная система, аппаратное обеспечение	неактуальная	Внешний нарушитель с высоким потенциалом не актуален для ИС
093	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).	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
094	Угроза несанкционированного управления синхронизацией и состоянием	Угроза заключается в возможности изменения нарушителем 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.), или в возможности модификации настроек и изменения режимов работы промышленных роботов, приводящих к вмешательству в производственный процесс и хищению хранящейся в памяти роботов информации (исходного кода, параметров продукции и др.). Данная угроза основана на слабостях механизма управления синхронизацией и состоянием, позволяющих нарушителю вносить изменения в его работу в определённые промежутки времени, или отсутствии механизмов аутентификации и авторизации.	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение	неактуальная	Технология управления синхронизацией и состоянием не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		Реализация данной угрозы возможна при условии наличия у нарушителя возможности: контролировать состояние дискредитируемого приложения (этапы выполнения алгоритма) или промышленных роботов; 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)				
095	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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-
096	Угроза несогласованности	Угроза заключается в возможности осуществления нарушителем деструктивных	ВнеН, ВнуН	Системное программное	неактуальная	Облачная технология не

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	политик безопасности элементов облачной инфраструктуры	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)		обеспечение, облачная система		применима для ИС
097	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 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	ВнуН	Хранилище больших данных	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		(например, одно средство защиты может отказать в доступе, а другое – предоставить доступ)				
098	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	ВнеН	Сетевой узел, сетевое программное обеспечение, сетевой трафик	актуальная	-
099	Угроза обнаружения хостов	Угроза заключается в возможности сканирования нарушителем вычислительной	ВнеН	Сетевой узел, сетевое	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		программное обеспечение, сетевой трафик		
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	ВнеН, ВнуН	Системное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнеС	Объекты файловой системы, аппаратное обеспечение, облачный сервер	неактуальная	Облачная технология не применима для ИС
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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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.)	ВнеН	Сетевой узел, сетевое программное обеспечение, сетевой трафик	актуальная	-
104	Угроза определения топологии вычислительной сети	Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы (т.н. сканирование сети) для получения сведений о топологии	ВнеН	Сетевой узел, сетевое программное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз. Данная угроза связана со слабостями 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		обеспечение, сетевой трафик		
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	ВнуН	Хранилище больших данных, метаданные	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнуН	Система хранения данных суперкомпьютера	неактуальная	Суперкомпьютерная технология не применима для ИС
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.).	ВнеВ, ВнуН	Системное программное обеспечение	неактуальная	Технология АСУ ТП не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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. 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;	ВнуН	Системное программное обеспечение, гипервизор	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		обновлений, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования; других инцидентов безопасности информации				
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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение, микропрограммное обеспечение, реестр	актуальная	-
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	ВнуН	Ресурсные центры грид-системы	неактуальная	Грид-технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
111	Угроза передачи данных по скрытым каналам	Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передаче управляющих команд 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), использования скрытых пикселей («пикселей отслеживания») и т.п. Данная угроза обусловлена недостаточностью мер защиты информации от утечки, а также контроля потоков данных. Реализация данной угрозы возможна при: наличии у нарушителя прав в дискредитируемой системе на установку специализированного программного обеспечения, реализующего функции внедрения в пакеты данных, формируемых для передачи в системе, собственной информации;	ВнеС, ВнуС	Сетевой узел, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		доступа к каналам передачи данных; посещении пользователем сайтов в сети Интернет и открытия электронных писем, содержащих скрытые пиксели				
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	ВнуН	Системное программное обеспечение, прикладное программное обеспечение	неактуальная	Технология АСУ ТП не применима для ИС
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	ВнеН, ВнуН	Системное программное обеспечение, аппаратное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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: наличие в системе открытых сессий работы пользователей; наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки				
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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		дискредитируемым приложением форматов входных (или обрабатываемых) данных; возможности взаимодействия с входным интерфейсом дискредитируемого приложения				
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.	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном («прослушивание» трафика) или активном (подмена пакетов, изменение их содержимого) режиме для сбора и анализа сведений (например, аутентификационной информации), 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 вычислительной сети; неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	ВнеН	Сетевой узел, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнеС, ВнуС	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-
118	Угроза перехвата привилегированного процесса	Угроза заключается в возможности получения нарушителем права управления процессом, обладающим высокими привилегиями (например, унаследованными от пользователя	ВнеС, ВнуС	Системное программное обеспечение, прикладное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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. 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		программное обеспечение, сетевое программное обеспечение		
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	ВнеС, ВнуС	Системное программное обеспечение, гипервизор, консоль управления гипервизором	неактуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеС, ВнуС	Информационная система, системное программное обеспечение	актуальная	Технология виртуализации не применима к ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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:	ВнеН, ВнуН	Объекты файловой системы, реестр	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		возникновения ошибок в работе отдельных процессов или всей операционной системы; наличии у нарушителя прав доступа к реестру или файлам, содержащим в себе данные реестра				
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	ВнеС, ВнуС	Системное программное обеспечение, сетевое программное обеспечение, информационная система	актуальная	-
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	ВнуН	Микропрограммное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		консолях BIOS/UEFI. Реализация данной угрозы возможна в одном из следующих случаев: 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				
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	ВнеН, ВнуН	Системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеН	Сетевой узел, сетевое программное обеспечение	неактуальная	Технология беспроводной связи не применима для ИС
126	Угроза подмены беспроводного клиента или точки доступа	Угроза заключается в возможности получения нарушителем аутентификационной или другой защищаемой информации, передаваемой в ходе автоматического подключения точек беспроводного доступа или клиентского программного обеспечения к доверенным субъектам сетевого взаимодействия,	ВнеН	Сетевой узел, сетевое программное обеспечение, аппаратное обеспечение, точка	неактуальная	Технология беспроводной связи не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		беспроводного доступа		
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	ВнеС	Прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-
128	Угроза подмены доверенного пользователя	Угроза заключается в возможности нарушителя выдавать себя за легитимного пользователя и выполнять приём/передачу данных от его имени.	ВнеН	Сетевой узел, сетевое	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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.		программное обеспечение		
129	Угроза подмены резервной копии программного обеспечения BIOS	Угроза заключается в возможности опосредованного внедрения нарушителем в BIOS/UEFI дискредитируемого компьютера вредоносного кода, путём ожидания 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	ВнуН	Микропрограммное и аппаратное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		BIOS/UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем)				
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	ВнеН	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	актуальная	-
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	ВнеС	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		«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				
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	ВнеС	Сетевой узел, сетевое программное обеспечение, сетевой трафик, прикладное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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.	ВнеН	Сетевой узел, метаданные	неактуальная	Технология беспроводной связи не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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. 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	ВнуС	Объекты файловой системы, информационная система, иммигрированная в облако	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнуН	Системное программное обеспечение, метаданные, объекты файловой системы	неактуальная	Облачная технология не применима для ИС
136	Угроза потери информации вследствие	Угроза заключается в возможности допуска ошибок при копировании защищаемой	ВнуН	Информационная система,	неактуальная	Технология больших

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	несогласованности работы узлов хранилища больших данных	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		узлы хранилища больших данных		данных не применима для ИС
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	ВнеВ	Сетевой трафик, объекты файловой системы	неактуальная	Облачная технология не применима для ИС. Внешний нарушитель с высоким потенциалом не актуален для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнуС	Информационная система, иммигрированная в облако, системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)				
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.)	ВнеС	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	актуальная	-
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	ВнеН, ВнуС	Информационная система, сетевой узел, системное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		системой или при использовании недостатков реализации сетевых протоколов. 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 и ошибками реализации сетевых протоколов. Реализация данной угрозы возможна при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы или наличия ошибок реализации сетевых протоколов (например, формирование IP-адреса версии 6 на основе MAC-адреса, определение доступности IP-адреса, использование функции контроля целостности PPP-интерфейса и др.)		программное обеспечение, сетевое программное обеспечение, сетевой трафик		
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	ВнуН	Информационная система, иммигрированная в облако, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик,	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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)		объекты файловой системы		
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	-	Системное программное обеспечение, аппаратное обеспечение, канал связи	неактуальная	Облачная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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 перезагрузки системы, а потребует проведения ремонтно-восстановительных работ. Данная угроза обусловлена наличием уязвимостей микропрограммного обеспечения средств хранения, обработки и (или) ввода/вывода/передачи информации, а также невозможности длительного нахождения средств хранения, обработки и (или) ввода/вывода/передачи информации в режиме предельно допустимых значений (частота системной шины, центрального процессора, количества обращений на чтение и/или запись и другие параметры). Реализация данной угрозы возможна при наличии у нарушителя прав на отправку команды или специально сформированных входных	ВнеС, ВнуС	Носитель информации, микропрограммное обеспечение, аппаратное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		данных на средства хранения, обработки и (или) ввода/вывода/передачи информации				
144	Угроза программного сброса пароля BIOS	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам BIOS/UEFI после перезагрузки компьютера 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	ВнуН	Микропрограммное обеспечение BIOS/UEFI, системное программное обеспечение	актуальная	-
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.	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеС, ВнуС	Вычислительные узлы суперкомпьютера, каналы передачи данных суперкомпьютера, системное	неактуальная	Суперкомпьютерная технология не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		программное обеспечение		
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	ВнуС	Ресурсные центры грид-системы, узлы грид-системы, грид-система, сетевое программное обеспечение	неактуальная	Грид-технология не применима для ИС
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»	-	Информационная система, система разграничения доступа хранилища	неактуальная	Технология больших данных не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		больших данных		
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. 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	ВнеС, ВнуС	Метаданные, объекты файловой системы, системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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)	ВнуС	Микропрограммное и аппаратное обеспечение BIOS/UEFI, каналы связи	актуальная	-
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	ВнеН	Сетевое программное обеспечение, сетевой узел	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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 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	ВнеН, ВнуН	Системное программное обеспечение, микропрограммное обеспечение, учётные данные пользователя	актуальная	-
153	Угроза усиления воздействия на вычислительные ресурсы пользователей	Угроза заключается в возможности осуществления нарушителем опосредованного деструктивного программного воздействия на дискредитируемую систему большим объёмом сетевого трафика, генерируемого сторонними	ВнеН, ВнуН	Информационная система, сетевой узел, системное программное	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	при помощи сторонних серверов	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		обеспечение, сетевое программное обеспечение		
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	ВнеС, ВнуС	Микропрограммное обеспечение BIOS/UEFI	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеН, ВнуН	Информационная система, сетевой узел, носитель информации, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнуН	Носитель информации	актуальная	-
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	ВнеН	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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.)				
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.	ВнеН, ВнуН	Носитель информации	актуальная	-
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	ВнеН	Сетевой узел, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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.)	ВнеН	Сервер, рабочая станция, носитель информации, аппаратное обеспечение	актуальная	-
161	Угроза чрезмерного использования	Угроза заключается в возможности возникновения ситуации типа «отказ в	ВнуН	Вычислительные узлы	неактуальная	Суперкомпьютерная

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями	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		суперкомпьютера		технология не применима для ИС
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	ВнеН, ВнуН	Системное программное обеспечение, прикладное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		программный код в дискредитируемый компьютер				
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 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	ВнеС, ВнуС	Системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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»	ВнеН, ВнуН	Облачная инфраструктура, созданная с использованием технологий виртуализации	неактуальная	Облачная технология не применима для ИС
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.	ВнуС	Программное обеспечение, техническое средство, информационная система, ключевая система информационной	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		Реализация данной угрозы возможна при условии выбора для применения в системе компонентов по цене, разрекламированности и др.		инфраструктуры		
166	Угроза внедрения системной избыточности	Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) 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)	ВнуС	Программное обеспечение, информационная система, ключевая система информационной инфраструктуры	актуальная	-
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	ВнуН	Сетевой узел, сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		антивирусного контроля на уровне организации. Реализация данной угрозы возможна при условии посещения пользователями системы с рабочих мест сайтов с неблагонадёжным содержимым				
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	ВнеН	Сетевое программное обеспечение	неактуальная	Технология доступа к сетевым сервисам (социальным сетям, облачным сервисам) с использованием неактивного/несуществующего адреса электронной почты не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		запись дискредитируемого пользователя для доступа к сетевым сервисам				
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). 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	ВнуС	Программное обеспечение, техническое средство	актуальная	-
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	ВнеН	Объект файловой системы	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнеН	Сетевой узел, сетевое программное обеспечение	актуальная	-
172	Угроза распространения «почтовых червей»	Угроза заключается в возможности нарушения безопасности защищаемой информации пользователя вредоносными программами, скрытно устанавливаемыми при получении пользователями системы электронных писем,	ВнеН	Сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		содержащих вредоносную программу типа «почтовый червь», а также невольного участия в 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				
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.	ВнеН	Сетевое программное обеспечение	актуальная	-
174	Угроза «фарминга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с	ВнеН	Рабочая станция,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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		сетевое программное обеспечение, сетевой трафик		
175	Угроза «фишинга»	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией (в т.ч. идентификации/аутентификации) пользователя путём убеждения его с помощью методов социальной инженерии (в т.ч. посылкой целевых писем (т.н. spear-phishing attack), с помощью звонков с вопросом об открытии вложения	ВнеН	Рабочая станция, сетевое программное обеспечение, сетевой трафик	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		письма, имитацией рекламных предложений (fake offers) или различных приложений (fake apps)) 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)				
176	Угроза нарушения технологического/производственного процесса из-за временны́х	Угроза заключается в возможности приведения системы в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в	ВнеН	Средство защиты информации	неактуальная	Технология АСУ ТП не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	задержек, вносимых средством защиты	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				
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,	ВнуН	Системное программное обеспечение, сетевое программное обеспечение, прикладное программное обеспечение, аппаратное обеспечение	неактуальная	Технология АСУ ТП не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		процедуры формирования временных пауз с возможностью выбора разных ответов (да/нет и т.п.). 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				
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	ВнеН, ВнуН	Системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнеН, ВнуН	Объекты файловой системы	актуальная	-
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, направленных на удалённое отключение/вывод из строя компонентов подсистемы обеспечения температурного режима	ВнеС, ВнуН	Технические средства воздушного кондиционирования, включая трубопроводные системы для циркуляции охлаждённого воздуха в ЦОД, программируемые логические контроллеры, распределённые системы контроля,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
				управленческие системы и другие программные средства контроля		
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	ВнеС	Одноразовые пароли	неактуальная	Технология использования одноразовых паролей не применима для ИС
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	ВнуН	Аппаратное средство	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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 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	ВнеВ, ВнуС	Программное обеспечение автоматизированной системы управления технологическими процессами	неактуальная	Технология АСУ ТП не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнуС	Мобильное устройство	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеН, ВнуН	Средство защиты информации	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
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	ВнуН	Сетевое программное обеспечение	актуальная	-
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	ВнеС, ВнуС	Средство защиты информации	актуальная	-
188	Угроза подмены программного обеспечения	Угроза заключается в возможности осуществления нарушителем внедрения в систему вредоносного программного	ВнуС	Прикладное программное обеспечение,	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		обеспечения за счёт загрузки и установки вредоносного программного обеспечения, скрытого под видом легитимного свободно распространяемого программного обеспечения. 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		сетевое программное обеспечение, системное программное обеспечение		
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	ВнеС	Системное программное обеспечение, сетевое программное обеспечение	актуальная	-
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	ВнеС	Сетевое программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Угроза заключается в возможности осуществления нарушителем заражения системы путем установки недоверенного 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	ВнеН, ВнуН	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	актуальная	-
192	Угроза использования уязвимых версий программного обеспечения	Угроза заключается в возможности осуществления нарушителем деструктивного воздействия на систему путём 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 или использованием	ВнеН, ВнуН	Прикладное программное обеспечение, сетевое программное обеспечение, системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		программного обеспечения, поддержка которого была прекращена производителем				
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Угроза заключается в возможности утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика, скрывающих сам факт передачи данных. Данная угроза 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	ВнеС	Информационные ресурсы, объекты файловой системы	актуальная	-
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	ВнеВ	Мобильное устройство	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС. Внешний нарушитель с высоким потенциалом не актуален для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	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	ВнеВ	Стационарные и мобильные устройства (компьютеры и ноутбуки) (аппаратное устройство)	неактуальная	Внешний нарушитель с высоким потенциалом не актуален для ИС
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	ВнеВ	Мобильное устройство (аппаратное устройство)	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС.

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				Внешний нарушитель с высоким потенциалом не актуален для ИС
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). Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт	ВнеС	Информация, хранящаяся на компьютере во временных файлах (программное обеспечение)	актуальная	-
198	Угроза скрытной регистрации вредоносной программой учетных	Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для	ВнеС	Система управления доступом, встроенная в	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	записей администраторов	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		операционную систему компьютера (программное обеспечение)		
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	ВнеС	Мобильное устройство и запущенные на нем приложения (программное обеспечение, аппаратное устройство)	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		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				
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	ВнеС	Данные пользователя мобильного устройства (аппаратное устройство)	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС
201	Угроза утечки пользовательских данных при	Угроза заключается в возможности утечки пользовательских данных за счет использования реализованной в браузерах функции	ВнеС	Аутентификационные данные пользователя	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	использовании функций автоматического заполнения аутентификационной информации в браузере	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		(программное обеспечение)		
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 (например, при попытке закрытия пользователем нежелательной рекламы). Реализация данной угрозы возможна при условии наличия на мобильном устройстве	ВнеС	Мобильные устройства (аппаратное устройство, программное обеспечение)	неактуальная	Технология, связанная с использованием мобильных устройств не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		вредоносной программы, способной запустить виртуальную машину и установить в эту виртуальную машину приложение				
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	ВнеС, ВнуС	Программное обеспечение	актуальная	-
204	Угроза несанкционированного изменения вредоносной	Угроза заключается в возможности несанкционированного изменения вредоносной программой значений параметров контроля и	ВнеС	Аппаратное устройство	неактуальная	Технология АСУ ТП не

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
	программой значений параметров программируемых логических контроллеров	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				применима для ИС
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	ВнеН	Аппаратное устройство, программное обеспечение	актуальная	-
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	ВнеВ	Аппаратное устройство	неактуальная	Технология АСУ ТП не применима для ИС. Внешний нарушитель с

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		пуско-наладочных работах. Угроза реализуется при условии перемещения оборудования с ЧПУ и приводит к невозможности его дальнейшей эксплуатации				высоким потенциалом не актуален для ИС
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	ВнеН, ВнуН	Аппаратное устройство, программное обеспечение	неактуальная	Технология АСУ ТП не применима для ИС
208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Угроза заключается в возможности использования вычислительных ресурсов средств вычислительной техники для осуществления сторонних вычислительных процессов. Угроза реализуется за счет внедрения в средства вычислительной техники вредоносной программы, содержащей код, реализующий использования вычислительных ресурсов для своих нужд (в частности, для майнинга криптовалюты). Данная угроза обусловлена недостаточностью следующих мер защиты информации: мер по антивирусной защите, что позволяет выполнить установку и запуск вредоносной	ВнеН, ВнеС, ВнуС, ВнуС	Средство вычислительной техники, мобильное устройство	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		программы; мер по ограничению программной среды, что позволяют нарушителю осуществлять бесконтрольный запуск программных компонентов.				
209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Угроза заключается в возможности получения доступа к защищенной памяти из программы, не обладающей соответствующими правами, в результате эксплуатации уязвимостей, позволяющих преодолеть механизм разграничения доступа, реализуемый центральным процессором. Реализация данной угрозы обусловлена наличием уязвимостей, связанных с ошибкой контроля доступа к памяти, основанных на спекулятивном выполнении инструкций процессора. Ошибка контроля доступа обусловлена следующими факторами: 1) отсутствие проверки прав доступа процесса к читаемым областям при спекулятивном выполнении операций, в том числе при чтении из оперативной памяти; 2) отсутствие очистки кэша от результатов ошибочного спекулятивного исполнения; 3) хранение данных ядра операционной системы в адресном пространстве процесса. Реализация данной угрозы возможна из-за наличия процессоров, имеющих аппаратные уязвимости и отсутствия соответствующих обновлений	ВнеН, ВнуН	Аппаратное устройство	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Угроза заключается в возможном нарушении функционирования программных, программно-аппаратных элементов информационной системы или информационной системы в целом из-за некорректной работы установленных обновлений (патчей) системного программного обеспечения. Угроза обусловлена наличием критических ошибок, дефектов, уязвимостей в используемом программном обеспечении информационной системы. Реализация данной угрозы возможна при условии установки обновлений на программно-аппаратные компоненты информационной системы	ВнуВ	Аппаратное устройство, микропрограммное, системное и прикладное программное обеспечение	неактуальная	Внутренний нарушитель с высоким потенциалом не актуален для ИС
211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечениям администрирования информационных систем	Угроза заключается в возможности деструктивного воздействия на информационную систему и обрабатываемую ею информацию в результате работы программного обеспечения, используемого для администрирования информационных систем. Данная угроза связана со слабостями процедуры проверки пользовательских данных, используемых при формировании конфигурационного файла для программного обеспечения администрирования информационных систем. Реализация данной угрозы возможна в случае, если в информационной системе используется программное обеспечение администрирования	ВнуН	Системное программное обеспечение	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		информационных систем, которое в качестве исходных данных использует конфигурационные файлы, сформированные на основе пользовательских данных				
212	Угроза перехвата управления информационной системой	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к информационным, программным и вычислительным ресурсам информационной системы в результате подмены средств централизованного управления информационной системой или её компонентами. Данная угроза обусловлена наличием у средств централизованного управления программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, возможностью несанкционированного доступа к данным средствам централизованного управления, а также недостаточностью мер по разграничению доступа к ним. Реализация данной угрозы возможна при условии наличия у нарушителя прав на осуществление взаимодействия со средствами централизованного управления	ВнуС	Инфраструктура информационных систем	актуальная	-
213	Угроза обхода многофакторной аутентификации	Угроза заключается в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода в дискредитируемую систему и компоненты,	ВнеВ	Системное программное обеспечение, микропрограм	неактуальная	Внешний нарушитель с высоким потенциалом

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		участвующие в процедуре многофакторной аутентификации. Данная угроза обусловлена: наличием уязвимостей программного обеспечения; слабостями мер антивирусной защиты и разграничения доступа. Реализация данной угрозы возможна: в случае работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников; при наличии у него привилегий установки программного обеспечения		мное обеспечение, учетные данные пользователя		не актуален для ИС
214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Угроза заключается в пропуске и/или значительной временной задержке определения (выявления) событий безопасности информации, что приводит к отсутствию реакции на попытки несанкционированного доступа в информационную (автоматизированную) систему, на внедрение вредоносных программ. Данная угроза обусловлена некорректной настройкой компонентов информационной (автоматизированной) системы и/или средств защиты информации, а также отсутствием таких компонентов и/или средств защиты информации. Реализация данной угрозы возможна при отсутствии мер защиты, связанных с мониторингом, сбором и анализом данных о событиях информационной безопасности	ВнуС	Программное обеспечение, каналы связи (передачи) данных	актуальная	-

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		(отсутствием мер регистрации событий безопасности)				
215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на дискредитируемую систему с использованием сторонних легитимных сервисов (социальных сетей, мессенджеров, репозиториев кода и т.п.), используемых в качестве посредника. Реализация данной угрозы возможна если дискредитируемая система уже скомпрометирована.	ВнеС	Программное обеспечение (программы)	неактуальная	Технология использования в качестве посредника сторонних легитимных сервисов (социальные сети, мессенджеры, репозитории) не применима для ИС
216	Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к приложениям, установленным на Smart-картах путем отправки специально сформированных команд управления (например, специально сформированных SMS-сообщений, отправленных на SIM-карту). Данная угроза обусловлена наличием уязвимостей в приложениях, устанавливаемых на Smart-карты. Реализация данной угрозы возможна при использовании Smart-карт типа Java Card	ВнеС	Программное обеспечение (программы)	неактуальная	Технология использования Smart-карт не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Угроза заключается в возможности внедрения вредоносного кода в информационную систему за счет использования скомпрометированных доверенных источников обновлений программного обеспечения. Реализация данной угрозы возможна при использовании скомпрометированных доверенных серверов обновлений программного обеспечения	ВнуС, ВнеС	Информационная система, файлы	актуальная	-
218	Угроза раскрытия информации о модели машинного обучения	Угроза заключается в возможности раскрытия нарушителем информации о модели машинного обучения, используемой в информационной (автоматизированной) системе. Данная угроза обусловлена слабостями разграничения доступа в информационных (автоматизированных) системах, использующих машинное обучение. Реализация данной угрозы возможна при наличии у нарушителя непосредственного доступа к модели машинного обучения	ВнеВ, ВнуС	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения	неактуальная	Технология машинного обучения не применима для ИС
219	Угроза хищения обучающих данных	Угроза заключается в возможности хищения нарушителем обучающих данных, используемых в информационной (автоматизированной) системе, реализующей технологии искусственного интеллекта. Данная угроза обусловлена слабостями разграничения доступа к обучающим данным, используемым в информационной (автоматизированной) системе. Реализация данной угрозы возможна при	ВнеС, ВнуС	Программное обеспечение (программы), использующее машинное обучение; обучающие данные машинного обучения	неактуальная	Технология машинного обучения не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		наличии у нарушителя непосредственного доступа к обучающим данным				
220	Угроза нарушения функционирования («обхода») средств, реализующих технологии искусственного интеллекта	Угроза заключается в возможности нарушения функционирования («обхода») нарушителем средств, реализующих технологии искусственного интеллекта. Данная угроза обусловлена следующими причинами: - отсутствие в обучающей выборке необходимых данных; - наличием недостатков модели машинного обучения;	ВнеВ, ВнуС	Программное обеспечение (программы), реализующие технологии искусственного интеллекта	неактуальная	Технология искусственного интеллекта не применима для ИС
221	Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных	Угроза заключается в возможности модификации (искажения) модели машинного обучения, используемой в информационной (автоматизированной) системе, реализующей технологии искусственного интеллекта. Данная угроза обусловлена: - недостатками реализации процесса машинного обучения; - недостатками устройства алгоритмов машинного обучения. Реализация данной угрозы возможна при наличии у нарушителя возможности воздействовать на процесс машинного обучения	ВнеВ, ВнуС	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения; обучающие данные машинного обучения	неактуальная	Технология машинного обучения не применима для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
222	Угроза подмены модели машинного обучения	Угроза заключается в возможности подмены нарушителем модели машинного обучения, используемой в информационной (автоматизированной) системе, реализующей технологии искусственного интеллекта. Данная угроза обусловлена слабостями разграничения доступа в информационных (автоматизированных) системах, использующих машинное обучение. Реализация данной угрозы возможна при наличии у нарушителя непосредственного доступа к модели машинного обучения	ВнуВ	Программное обеспечение (программы), использующее машинное обучение; модели машинного обучения	неактуальная	Технология машинного обучения не применима для ИС. Внутренний нарушитель с высоким потенциалом не актуален для ИС
ТКУ.1	Угроза утечки акустической (речевой) информации	Угроза заключается в возможности перехвата злоумышленником голосового воспроизведения пользователями и обслуживающим персоналом информации, обрабатываемой в ИС. Реализация данной угрозы возможна путем подслушивания переговоров нарушителем, находящимся в непосредственной близости с помещением, в котором ведутся переговоры.	ВнеС; ВнуС; ВнеН; ВнуН	Акустическая (речевая) информация	актуальная	
ТКУ.2	Угроза утечки акустической (речевой) информации с помощью специализированных средств	Угроза заключается в возможности перехвата злоумышленником голосового воспроизведения пользователями и обслуживающим персоналом информации, обрабатываемой в ИС. Реализация данной угрозы возможна с помощью использования злоумышленником специальной аппаратурой для съема речевой информации.	ВнеВ; ВнуВ	Акустическая (речевая) информация	неактуальная	Внутренний и внешний нарушители с высоким потенциалом не актуальны для ИС
ТКУ.3	Угроза утечки видовой информации	Угроза заключается в возможности перехвата злоумышленником видовой информации с помощью просмотра обрабатываемой	ВнеС; ВнуС;	Видовая информация	актуальная	

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		информации с экранов дисплеев и других устройств отображения средств вычислительной техники, входящих в состав информационной системы. Реализация данной угрозы возможна путем непосредственного наблюдения в служебных помещениях, либо вне помещения с расстояния прямой видимости с использованием оптических средств.	ВнеН; ВнуН			
ТКУ.4	Угроза утечки видовой информации с помощью специализированных средств	Угроза заключается в возможности перехвата злоумышленником видовой информации с помощью просмотра обрабатываемой информации с экранов дисплеев и других устройств отображения средств вычислительной техники, входящих в состав информационной системы. Реализация данной угрозы возможна с помощью использования злоумышленником специальных электронных средств съема видовой информации.	ВнеВ; ВнуВ	Видовая информация	неактуальная	Внутренний и внешний нарушители с высоким потенциалом не актуальны для ИС
ТКУ.5	Угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	Угроза заключается в возможности перехвата злоумышленником информации с помощью каналов побочных электромагнитных излучений и наводок (ПЭМИН). Реализация данной угрозы возможна с помощью специальных средств регистрации, перехвата и съема побочных информативных электромагнитных полей, и электрических сигналов, возникающих при обработке	ВнеВ; ВнуВ	Побочные информативные электромагнитные поля, и электрические сигналы, возникающие при обработке информации	неактуальная	Внутренний и внешний нарушители с высоким потенциалом не актуальны для ИС

Идентификатор УБИ	Наименование УБИ	Описание УБИ	Источник УБИ (тип и потенциал нарушителя)	Объект воздействия	Актуальность УБИ	Примечание
		информации техническими средствами, входящими в состав ИС		техническими средствами		
ТКУ.6	Угрозы безопасности информации техногенных, стихийных и антропогенных источников	Техногенные источники угроз могут являться причиной отказов или сбоев в работе технических средств или программного обеспечения и напрямую зависят от таких свойств технических средств и программного обеспечения, как надежность и отказоустойчивость. Для ИС угрозы, связанные с действием стихийных источников, могут привести к нарушению целостности и доступности обрабатываемой в системе информации. Последствия в результате действия антропогенных источников угроз могут привести к нарушению конфиденциальности, целостности и доступности обрабатываемой в ИС информации.	ВнеС; ВнуС; ВнеН; ВнуН	Технические средства обработки информации, программное обеспечение	актуальная	-

Лист регистрации изменений

Изм	новых				Всего листов (страниц) в докум.	№ документа	Входящий номер сопроводи-тельного документа и дата	Подпись	Дата
	измененных	замененных	новых	изъятых					

Подп. и дата

Взам. инв. №

Инв. № дубл.

Подп. и дата

Инв. № подп

Лит	Изм.	№ докум.	Подп.	Дата

Лист